FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

SISTEMA DE INSTRUMENTAÇÃO DISTRIBUÍDA SUPORTADO POR REDE SEM FIOS

Isabel Maria Gonçalves Fernandes Vaz Pinheiro

Licenciada em Engenharia Electrotécnica

pelo Instituto Superior de Engenharia do Porto

Dissertação submetida para satisfação parcial dos requisitos de grau de Mestre

em Engenharia Electrotécnica e de Computadores

(Área de especialização de Automação Industrial)

Dissertação realizada sob a orientação de:

Professor Doutor Adriano da Silva Carvalho,

do Departamento de Engenharia Electrotécnica e de Computadores

da Faculdade de Engenharia da Universidade do Porto

Porto, 2008

Em memória do meu Pai

e dos meus Padrinhos

Aos meus filhos

Isabel e Diogo

Agradecimentos

A realização deste trabalho apenas foi possível devido ao empenhamento, dedicação e apoio de muitas pessoas. Algumas delas merecem uma menção especial.

O meu orientador, Professor Adriano da Silva Carvalho, não só pelo apoio, incentivo e disponibilidade constantemente manifestada, mas pela confiança em mim depositada, guiando-me com o seu saber, experiência, competência e rigor profissional, durante o trabalho de investigação, sempre na direcção correcta. Sem ele a realização desta dissertação não teria sido possível.

Todos os meus familiares e amigos que, directa ou indirectamente, contribuíram para tornar este trabalho realidade.

De um modo especial, os meus filhos adorados, o sol da minha vida, que muitas vezes sentiram a minha ausência durante a elaboração desta tese. O meu marido, o meu grande companheiro e amigo, cuja colaboração e incentivo foram essenciais para me manter sempre com vontade de continuar. Finalmente, a minha mãe, a melhor mãe do mundo, que sempre me apoiou incondicionalmente, não só durante a realização deste trabalho, mas ao longo de toda a minha vida.

Resumo

As redes de campo são utilizadas numa grande variedade de domínios de aplicação, tais como na automação industrial, indústria de processos, automação de edifícios, aplicações da indústria automóvel, controlo ferroviário, controlo aéreo e controlo de subestações eléctricas. Algumas das vantagens que este tipo de redes introduziu no chão de fábrica são: a flexibilidade, a melhoria no desempenho do sistema e a simplificação, tanto na instalação do sistema, como na posterior manutenção e actualização.

Uma tecnologia cuja aplicação no chão de fábrica está a ser amplamente estudada é a comunicação sem fios. Sendo já uma realidade a proliferação de redes sem fios, importa desenvolver aplicações fiáveis que utilizem este tipo de tecnologia, de forma a poder aproveitar as suas características de mobilidade e baixo consumo.

Esta tese propõe a implementação de um sistema de instrumentação distribuída suportado por uma rede sem fios. Assim, numa primeira parte é apresentado o estado da arte das redes de comunicação industriais, sendo de seguida analisadas as tecnologias de comunicação sem fios. Numa segunda parte é implementado o sistema proposto, baseado no *standard* IEEE 802.15.4/Zigbee. Por último, são analisados os resultados obtidos no trabalho implementado, sendo ainda abordadas algumas perspectivas para desenvolvimentos futuros.

Abstract

Fieldbuses are used in a wide variety of application domains, such as industrial automation, process industry, home and building automation, automobile industry, as well as railroad, aircraft and electrical substations control. Some of the advantages brought by fieldbuses into factory floor are: flexibility, improvement on the system performance and simplification, not only during installation but also when maintenance and update are needed.

A technology whose application on the ground floor is being widely investigated is wireless communication. The emergency of wireless networks is already a reality, it is thus evident that the next important step is the development of reliable applications supported on such technology, in order to take advantage of its characteristics of mobility and energetic efficiency.

This Thesis proposes the implementation of a distributed instrumentation system based on a wireless technology. In an initial phase is presented the state of the art of industrial communications, next are presented the wireless standards. Finally, the results obtained with the implemented system are analyzed, as well as some perspectives for future developments.

Índice

Índice de Figuras

Índice de Tabelas

Acrónimos

ACL	Asynchronous Connectionless Link
ADC	Analogical Digital Converter
AES	Advanced Encryption Protocol
AF	Application Framework
AFH	Adaptive Frequency Hopping
AIB	Application Support sub Layer Information Base
AP	Access Point
APDU	Application Protocol Data Unit
APL	Application Layer
APS	Application Support Sub Layer
APSDE	Application Support Sub Layer Data Entity
APSDE - SAP	Application Support Sub Layer Data Entity - Service Access Point
APSME	Application Support Sub Layer Management Entity
APSME - SAP	Application Support Sub Layer Management Entity - Service Access Point
ARQ	Automatic Repeat reQuest
AS	Application Server
ASDU	APS Service Data Unit
ASE	Application Service Element
ASnd	Asynchronous data
AT	Answer Telegram
BSS	Basic Service Set
CAC	Channel Access Code
CAMAC	Computer Automated Measurement And Control
CAP	Contention Access Period
CBA	Component Based Automation
CCA	Clear Channel Assessment

CCITT	Commité Consultatif International de Telegraphique et Telephonique
CCK	Complementary Code Keying
CFP	Contention Free Period
CIM	Computer Integrated Manufacturing
CIP	Common Interface Protocol
CN	Controlled Node
CORBA	Common Object Request Broker Architecture
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA - CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA - CD	Carrier Sense Multiple Access with Collision Detection
CST	Composite State Protocol
CVSD	Continuous Variable Slope Delta
DAC	Device Access Code
DCF	Distributed Coordination Function
DCOM	Distributed Component Object Model
DCS	Distributed Control System
DDC	Direct Digital Control
DE	Data Entity
DFS	Dynamic Frequency Selection
DMA	Direct Memory Access
DPSK	Differential Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
ECU	Electronic Control Unit
EPA	Ethernet for Plant Automation
EPL	Ethernet Power Link
ERP	Enterprise Resource Planning
ESS	Extended Service Set
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction

FF	Fieldbus Foundation
FFD	Full Function Device
FHSS	Frequency Hopping Spread Spectrum
FIP	Factory Instrumentation Protocol
GAP	General Access Profile
GAP	General Access Profile
GFSK	Gaussian Frequency Shift Keying
GTS	Guaranteed Time Slots
HCI	Host Controller Interface
HCI	Host Controller Interface
HSE	High Speed Ethernet
HTTP	Hypertext Transfer Protocol
I&D	Investigação e Desenvolvimento
IAC	Inquiry Access Code
IAPP	Inter Access Point Protocol
IBSS	Independent BSS
IDA	Interface for Distributed Automation
IE	Industrial Ethernet
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IR	InfraRed
IRT	Isochronous Real Time
ISA	International Society of Automation
ISM	Industrial, Scientific And Medical
ISO	International Organization for Standardization
ISP	Interoperable System Project
L2CAP	Logical Link Control And Adaptation Layer Protocol
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
LLC	Logical Link Control
LM	Link Manager
LMP	Link Manager Protocol

LQI	Link Quality Indicator
MAC	Medium Access Control
MAP	Manufacturing Automation Protocol
MCPS - SAP	Medium Access Control Common Part Sub Layer - Service Access Point
MDT	Master Data Telegram
ME	Management Entity
MES	Manufacturing Execution System
MIL - STD	Military STandarD
MIMO	Multiple Input, Multiple Output
MLME - SAP	Medium Access Control Management Entity Sub Layer - Service Access Point
MMI	Man Machine Interface
MMS	Manufacturing Message Specification
MN	Managing Node
MPS	Manufacturing Periodic/Aperiodic Services
MT	Monitor Test
NIB	Network Layer Information Base
NLDE	Network Layer Data Entity
NLDE - SAP	Network Layer Data Entity - Service Access Point
NLME	Network Layer Management Entity
NLME - SAP	Network Layer Management Entity - Service Access Point
NPDU	Network Layer Protocol Data Unit
NRT	Non Real Time
NSDU	Network Service Data Unit
ODVA	Open Devicenet Vendor Association
OFDM	Orthogonal Frequency Division Multiplexing
OPC	Object linking and embedding for Process Control
OSAL	Operating System Abstraction Layer
OSI	Open Systems Interconnection
PAN	Personal Area Network
PC	Personal Computer
PCF	Point Coordination Function
PD - SAP	Physical Layer Data - Service Access Point
PDU	Protocol Data Units

PID	Proportional Integral Derivative
PLC	Programmable Logic Controller
PLME - SAP	Physical Layer Management Entity - Service Access Point
PPDU	Physical layer Protocol Data Unit
PPTP	Point to Point Tunnelling Protocol
PReq	Poll Request
PRes	Poll Response
PRNG	Pseudo Random Number Generator
PROFIBUS	PROcess Field BUS
PSDU	Physical layer Service Data Unit
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RF	Radio Frequency
RFD	Reduced Function Device
RFD	Reduced Function Device
RPC	Remote Procedure Call
RSSI	Received Signal Strength Indication
RT	Real Time
RTE	Real Time Ethernet
RTP	Real Time and reliable datagram Protocol
RTPS	Real Time Publisher Subscriber
SAP	Service Access Point
SCADA	Supervisory Control And Data Acquisition
SCNM	Slot Communication Network Management
SCO	Synchronous Connection Oriented
SDAP	Service Discovery Application Profile
SDP	Service Discovery Protocol
SERCOS	SErial Realtime COmmunications System
SIG	Special Interest Group
SMTP	Simple Mail Transfer Protocol

SoA	Start of Asynchronous
SoC	Start of Cycle
SOC	System On Chip
SOC-BB	System On Chip – Battery Board
SSID	Service Set IDentifier
SSP	Security Services Provider
TCNet	Time Critical control network
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TKIP	Temporal Key Integrity Protocol
TOP	Technical Office Protocol
TPC	Transmit Power Control
TXOP	Transmission Opportunity
UDP	User Datagram Protocol
USART	Universal Synchronous Asynchronous Receiver Transmitter
USB	Universal Serial Bus
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WEP	Wired Equivalent Protocol
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
XML	eXtensible Markup Language
ZDO	Zigbee Device Object

1 Introdução

Uma das principais razões para a emergência das redes de campo (*fieldbuses*) foi a necessidade de substituição das ligações ponto a ponto por um único barramento. As redes de campo são tipicamente redes que ligam componentes de campo, como sensores e actuadores, a controladores, como por exemplo PLCs (Programmable Logic Controllers) na automação industrial, ou ECUs (Electronic Control Units) em aplicações do ramo automóvel.

As redes de campo são utilizadas numa grande variedade de domínios de aplicação, tais como na automação industrial, indústria de processos, automação de edifícios, aplicações da indústria automóvel, controlo ferroviário, controlo aéreo, controlo de subestações eléctricas, etc.

Algumas das vantagens que este tipo de redes introduziu no chão de fábrica são: a flexibilidade, a melhoria no desempenho do sistema e a simplificação, tanto na instalação do sistema, como na posterior manutenção e actualização.

Devido à natureza dos requisitos de comunicação impostos pelas comunicações, as redes de campo têm taxas de transmissão baixas, pacotes de dados pequenos e tipicamente requerem características de tempo real que exigem o determinismo da transferência de dados.

As redes de campo têm a sua origem nos finais dos anos 60, na altura do domínio da instrumentação nuclear, com o *standard* CAMAC (Computer Automated Measurement and Control) e no início dos anos 70, nas aplicações aeronáuticas e aeroespaciais, com o *standard* MIL-STD-1553 (MILitary STandarD). No entanto, foi a área da automação industrial a responsável pela maior parte dos desenvolvimentos das redes de campo.

A necessidade de integração de sistemas heterogéneos, difícil na altura devido à falta de *standards*, resultou em duas grandes iniciativas. Estas duas iniciativas foram os projectos dos protocolos TOP (Technical Office Protocol) e MAP (Manufacturing Automation Protocol). Estes dois projectos expuseram algumas falhas nas implementações da *stack* de sete níveis do modelo OSI (Open Systems Interconnection), no contexto das

aplicações na automação industrial. Como resultado, tipicamente apenas o nível um (nível fisico), o dois (nível de ligação de dados) e o sete (aplicação) são utilizados nas redes de campo, tal como especificado no *standard* internacional das redes de campo IEC 61158 (International Electrotechnical Commission). Este *standard* recomenda a inclusão das funções dos níveis 3 e 4, ou no nível 2 ou no 7, sendo as funções dos níveis 5 e 6 incluídas no nível 7.

A Ethernet, tecnologia fundamental nas redes administrativas, está cada vez mais a ser adoptada na comunicação industrial e até mesmo ao nível das redes de campo. O CSMA/CD (Carrier Sense Multiple Access With Collision Detection) tem vindo a ser substituído por outros mecanismos que permitem o comportamento determinístico requerido nas comunicações em tempo real, de forma a suportar *deadlines* de tempo real e sincronização de actividades. Uma variedade de soluções foi proposta, para que esse objectivo fosse atingido.

Outra tecnologia cuja aplicação no chão de fábrica está a ser amplamente estudada é a comunicação sem fios. Esta tecnologia, não só permite uma maior flexibilidade na instalação, manutenção e actualização dos sistemas, como suprime os problemas devidos à cablagem. No entanto, um sistema de comunicação sem fios, para operar no chão de fábrica de um modo eficiente, tem de garantir uma alta fiabilidade, um baixo e previsível atraso na transferência de dados (tipicamente abaixo dos 10 ms para aplicações em tempo real), tem de suportar um grande número de sensores e de actuadores e ter um baixo consumo, de forma a possibilitar uma alimentação sem fios, o que permite um sistema totalmente independente de fios, tanto na comunicação como na alimentação.

Este tipo de tecnologia não tem tido uma boa aceitação no chão de fábrica, devido à dificuldade em garantir algumas das características acima mencionadas. Nos ambientes industriais os factores que contribuem para a degradação dos canais de comunicação sem fios são essencialmente devidos à presença de motores eléctricos e de uma variedade de equipamentos que provocam descargas eléctricas, o que contribui para um nível ainda mais elevado de erros nos bits e de perdas de pacotes de dados neste tipo de redes. A melhoria da qualidade do canal de comunicação e o desenvolvimento de aplicações robustas e tolerantes a perdas são aspectos que têm sido sujeitos de extensas investigações e desenvolvimentos, cujo objectivo é a diminuição dos problemas típicos deste tipo de redes.

Sendo já uma realidade a proliferação de redes sem fios, importa desenvolver aplicações fiáveis que utilizem este tipo de tecnologia, de forma a poder aproveitar as suas características de mobilidade e baixo consumo.

Assim, o objectivo desta dissertação é o estudo do estado da arte das redes de comunicação industriais, dando particular destaque aos *standards wireless*, tendo em vista a aplicação de um *standard* deste tipo, o IEEE 802.15.4/Zigbee, para o desenvolvimento de um sistema de instrumentação distribuída suportado numa rede sem fios.

No capítulo 2, Redes de Comunicações Industriais, é abordado o estado da arte das redes de comunicações industriais, sendo feito um resumo desde o seu aparecimento até à actualidade.

No capítulo 3, Redes de comunicações sem fios, não só é abordado o estado da arte das redes de comunicações *wireless*, como são descritos os *standards* mais implementados, com vista à escolha do *standard* a ser utilizado no projecto.

No capítulo 4, Sistema de Instrumentação distribuída suportado em comunicação sem fios, é apresentado o trabalho desenvolvido, baseado no *standard* de comunicação sem fios IEEE 802.15.4/*Zigbee* e na plataforma de *hardware* CC2431 da Chipcon/Texas Instruments.

No capítulo 5, Conclusões, é feita uma análise aos resultados obtidos no trabalho implementado e à exequibilidade de redes de campo suportadas por tecnologias sem fios, sendo ainda abordadas algumas perspectivas para desenvolvimentos futuros.

2 Redes de Comunicações Industriais

2.1 Introdução

A evolução da tecnologia nos últimos anos teve uma grande influência na sociedade, levando a caracterizá-la hoje como a sociedade do conhecimento. Com efeito, a globalização é hoje uma realidade, permitindo um rápido acesso à informação onde quer que ela se encontre, originando assim um esforço de actualização constante, já que a informação de que hoje dispomos ficará rapidamente ultrapassada.

O reflexo nas empresas fabris desta maneira de estar da sociedade actual traduz-se em novos desafios, no que respeita à produtividade: o nível de exigência do consumidor aumentou, os ciclos de vida dos produtos diminuíram, as linhas de produção tiveram de ser optimizadas em termos de níveis de *stocks* e flexibilidade, tudo a um baixo custo, para ser possível responder às necessidades do mercado de uma forma rentável. Este desafio nas áreas da inovação e da competitividade obrigou as empresas a concentrar esforços na modernização tecnológica dos seus processos de fabrico, nomeadamente na automatização dos mesmos. Deste esforço integrado resultaram, para além de produtos mais competitivos, o desenvolvimento de soluções tecnológicas avançadas que, à medida que se tornaram cada vez mais comuns e acessíveis, passaram também a ser incorporadas nos próprios processos de fabrico.

Durante as últimas três décadas assistiu-se a uma evolução sem paralelo na área dos sistemas de controlo, nomeadamente ao nível dos respectivos processos de concepção, implementação e operação. Isto deveu-se, em grande parte, aos novos desenvolvimentos, quer em áreas tecnológicas, tais como a microelectrónica e as telecomunicações, quer em áreas associadas à gestão e à integração de sistemas, bem como ao desejo de disponibilizar aos utilizadores finais equipamentos com maiores funcionalidades a custos mais reduzidos.

Este desenvolvimento reflectiu-se também ao nível das comunicações industriais, através da substituição progressiva das tradicionais comunicações ponto-a-ponto pelas

LANs (*Local Area Networks*). Embora inicialmente os motivos desta mudança estivessem relacionados com aspectos económicos, tais como a redução da cablagem e dos custos de manutenção, resultaram posteriormente em enormes vantagens ao nível da descentralização do controlo dos processos, na facilidade de instalação e configuração, na elevada flexibilidade de utilização e na melhoria do desempenho dos sistemas de controlo.

A crescente descentralização ao nível das funções de controlo e a crescente utilização de dispositivos inteligentes baseados em microprocessadores ou microcontroladores, criaram as condições necessárias para o desenvolvimento e proliferação das redes de campo. Estas são um tipo específico de rede local industrial, com o objectivo de interligar controladores, sensores e actuadores, que realizam a *interface* com o processo industrial.

Neste capítulo são analisadas as redes de comunicações industriais, com destaque para as redes de campo, os seus *standards* e as soluções comerciais ao nível das redes com fios. Neste contexto, na secção 1.2 é abordado o sistema de controlo do ambiente industrial, sendo ainda feito um resumo sobre a evolução das tecnologias de controlo. Na secção 1.3 é feita uma descrição do modelo OSI, uma vez que os *standards* de redes de campo são baseados nesse modelo. De seguida, na secção 1.4 é analisada a arquitectura das comunicações industriais, sendo ainda estabelecida uma relação entre esta e os níveis de controlo existentes num ambiente industrial. Na secção 1.5 são abordadas as redes de campo em particular, é feito um breve resumo sobre a história da standardização deste tipo de redes e são ainda apresentados os protocolos incluídos no conjunto de *standards* que especificam este tipo de redes. Por último, na secção 1.6 é abordada a *Ethernet* em tempo real e são apresentadas as soluções RTE (Real Time Ethernet) existentes.

2.2 O Sistema de controlo

O funcionamento de forma correcta e segura de um processo industrial de qualquer natureza é assegurado por intermédio de um sistema de controlo apropriado. Independentemente da dimensão ou da complexidade do processo em causa, o respectivo sistema de controlo pode ser decomposto em três subsistemas com funções bem definidas: o processo controlado, o controlador e o operador humano (Figura 2.1) [5].

Figura 2.1 - Sistema de controlo

O controlador é um equipamento que interage com o seu ambiente através de duas *interfaces* com características distintas:

- a *interface* com o processo controlado é definida como a *interface* de instrumentação;
- a *interface* com o operador humano é definida como a *interface* homem-máquina.
- A *interface* de instrumentação consiste num conjunto de sensores e actuadores que transformam os sinais físicos do processo controlado em sinais com características apropriadas para serem utilizados pelo controlador, e vice-versa. A *interface* homem-máquina consiste num conjunto de dispositivos de entrada e saída, que permitem a interacção com um operador humano. Tipicamente, esta interacção realiza-se ao nível da definição de parâmetros do processo e da supervisão da respectiva evolução.

A função do controlador é controlar a evolução do processo através da execução de um algoritmo de controlo adequado. A partir do processamento da informação obtida, quer directamente do estado do processo através da *interface* de instrumentação, quer fornecida pelo operador humano através da *interface* homem-máquina, o algoritmo de controlo produz um conjunto de comandos que são enviados para o processo através da *interface* de instrumentação. Para realizar estas funções o controlador dispõe de uma estrutura funcional, baseada na utilização de equipamentos adequados ao processo em causa, que suporta a execução do algoritmo de controlo.

Ao nível da estrutura funcional, estes sistemas de controlo podem ser classificados em três tipos de arquitecturas (Figura 2.2) [5].

- Centralizadas - o algoritmo de controlo é executado por um único equipamento;
- Descentralizadas - o algoritmo é executado num único equipamento, mas

algumas tarefas de processamento mais simples (ex. condicionamento e aquisição de sinais) são executadas por outros equipamentos de menor complexidade. Isto implica a existência de uma estrutura de comunicações que permita a interacção e a cooperação entre os vários equipamentos (ex. comunicações série ponto-a-ponto);

- Distribuídas - o algoritmo de controlo encontra-se distribuído por vários equipamentos de complexidade e natureza distintas. Tal como nas arquitecturas descentralizadas, é também necessário dispor de uma estrutura de comunicações adequada, sendo esta, contudo, comparativamente muito mais complexa (ex. rede de campo).

Figura 2.2 - Exemplos de arquitecturas de controlo

2.2.1 Evolução das Tecnologias de Controlo

O advento do computador no início dos anos 60 permitiu que estes passassem também a ser utilizados para implementar funções de controlo. O termo DCC (Direct Digital Control) foi utilizado na época para enfatizar o facto do controlo do processo ser realizado directamente pelo computador. O facto de serem programáveis proporcionou-lhes uma esmagadora vantagem em comparação com as tecnologias de lógica discreta utilizadas até ao momento. Um único equipamento (um computador) concentra em si, quer

as tarefas do controlador, quer as *interfaces* de instrumentação e de homem-máquina. No caso da *interface* de instrumentação, os sensores e actuadores são tipicamente ligados ao controlador através de ligações ponto-a-ponto analógicas (ex. anel de corrente). Em paralelo com este processo, tem também início nos finais do anos 60 o desenvolvimento de máquinas de controlo numérico e de *robots* industriais.

As arquitecturas de controlo desenvolvidas até esta época são essencialmente centralizadas. Contudo, as crescentes exigências da indústria, conjugadas com o desenvolvimento do microprocessador no início dos anos 70, permitiram uma evolução para as primeiras arquitecturas descentralizadas. Esta evolução efectuou-se segundo duas perspectivas [6]:

- uma ao nível das indústrias de processos, com o desenvolvimento dos DCS (Distributed Control Systems) com o objectivo de interligar hierarquicamente os equipamentos de controlo de menor complexidade (por exemplo controladores PID - Proportional Integral Derivative) aos equipamentos de maior complexidade (por exemplo mini-computadores);
- outra ao nível das indústrias de manufactura, onde o PLC, cujo desenvolvimento se deu no início dos anos 70, foi utilizado como elemento central das arquitecturas de controlo.

Em ambas as perspectivas, a interligação entre equipamentos era tipicamente realizada, quer através de ligações ponto-a-ponto analógicas, quer através de ligações digitais, utilizando neste último caso protocolos de comunicação proprietários. Embora esta evolução tenha permitido o desenvolvimento de sistemas de controlo cada vez mais complexos, durante a primeira década da sua utilização, as arquitecturas de controlo continuaram a ser caracterizadas por uma estrutura tipicamente centralizada e só mais tarde se registou uma evolução para soluções do tipo descentralizado.

Entre meados dos anos 80 e inícios dos 90, assistiu-se a uma alteração da estrutura das arquitecturas de controlo através da crescente utilização de redes de comunicação industriais para interligar os equipamentos de controlo. Esta evolução tecnológica foi o ponto de partida das primeiras arquitecturas de controlo descentralizadas baseadas numa estrutura de comunicações digital. Estas arquitecturas, embora mais complexas, permitiram obter um importante conjunto de vantagens, das quais se destacam: menores custos, melhores desempenhos, instalação e manutenção mais simples, modularidade, facilidade

na detecção de erros e avarias, etc. Na sequência desta evolução, surge também nesta época o conceito de CIM (Computer Integrated Manufacturing).

O CIM visa a cooperação entre os diferentes sistemas intervenientes no ambiente de fabrico e engloba todas as actividades com ele relacionadas, desde o projecto e desenvolvimento até ao *marketing* e vendas, passando pelo controlo do fabrico. Para que essa cooperação exista de facto é necessário que haja integração entre os sistemas. A integração significa a possibilidade de os subsistemas da empresa poderem interactuar entre si através de sistemas de comunicações de dados e bases de dados comuns.

Os sistemas de comunicações requerem infraestruturas técnicas (*software* e *hardware*). As comunicações requerem também regras (protocolos), regras essas condicionadas, não apenas por aspectos técnicos, mas também pela funcionalidade exigida.

Uma das representações da filosofia CIM consiste em decompor a empresa em cinco níveis, tal como a figura 2.3 indica.

Figura 2.3 - Representação da filosofia CIM

A subdivisão em níveis é baseada, entre outros aspectos, nos tipos de actividades realizadas na empresa e leva, geralmente, ao uso de diferentes tipos de redes de comunicações nos vários níveis.

No interior de cada nível as comunicações horizontais são geralmente asseguradas por uma rede local. As comunicações verticais entre dois níveis adjacentes são resolvidas interligando as redes através de dispositivos de ligação.

A figura 2.4 representa um exemplo de uma arquitectura possível para a hierarquia de comunicações dentro de uma empresa.

Nos níveis superiores da hierarquia as comunicações podem ser caracterizadas como correspondendo à troca de grandes quantidades de informação, que tem de ser processada durante períodos relativamente longos mas com uma frequência relativamente baixa.

Ao contrário, nos níveis inferiores da hierarquia pequenas quantidades de informação precisam de ser processadas de uma forma rápida, com o objectivo de controlar processos industriais em tempo real. Este tipo de transacções tem normalmente uma periodicidade cíclica e uma frequência relativamente elevada.

Pode-se então concluir que não é possível satisfazer todos estes requisitos de transferência de dados com um só tipo de rede.

Figura 2.4 - Representação de uma arquitectura possível para a hierarquia das comunicações de uma empresa

Pode assim propor-se uma classificação hierárquica das comunicações industriais em três grandes grupos, que são: redes de fábrica, redes de célula e redes de campo.

As redes de fábrica abrangem os níveis superiores da hierarquia, enquanto as redes de campo correspondem ao nível mais baixo.

Embora esta evolução abrisse um conjunto enorme de perspectivas ao nível da integração de equipamentos situados em diferentes níveis de controlo, na prática isto acabou por não se verificar, devido ao desenvolvimento de muitas soluções proprietárias. Estas acabaram por limitar as potencialidades das arquitecturas de controlo, nomeadamente

ao nível da integração e da interoperabilidade entre equipamentos. Este problema colocou-se de forma especialmente grave ao nível das redes de campo, com os diferentes fabricantes a tentar impor as suas soluções como o *standard* a utilizar. São alguns exemplos o (PROcess FIeld BUS), o WorldFIP (Factory Instrumentation Protocol), o DeviceNet, o INTERBUS-S, e o AS-Interface (Application Server). Este processo terminou apenas recentemente através da adopção de uma solução de compromisso entre as várias propostas existentes [7]. Ao nível das arquitecturas de controlo registou-se uma tendência para adoptar soluções distribuídas, não só devido à possibilidade de dispor de equipamentos com maiores capacidades de processamento, mas também através do desenvolvimento de arquitecturas de comunicação que suportam elevados níveis de integração entre equipamentos.

Embora a introdução das redes industriais viesse resolver o problema da integração horizontal de equipamentos (situados no mesmo nível de controlo), a integração vertical (entre níveis de controlo) foi sempre um problema em aberto. As soluções apontadas inicialmente passavam pela utilização de equipamentos dedicados (*gateways*) ou pelo desenvolvimento de *software* específico que implementava as tarefas de mapear os serviços de comunicação das diferentes redes. Como estas soluções eram normalmente caras e complexas, surgiu no final dos anos 80 a ideia de desenvolver uma arquitectura de comunicações aberta baseada na estrutura do modelo OSI (*Open Systems Interconnection*). Exemplos destas soluções foram o MAP (Manufacturing Automation Protocol) e o MMS (Manufacturing Message Specification). No entanto, o seu sucesso acabou por ser limitado devido, quer à falta de suporte tecnológico adequado, quer à cumplicidade das soluções propostas.

Em paralelo, nas indústrias de processos a utilização de tecnologias SCADA (Supervisory Control and Data Aquisition) foi vista como uma alternativa mais simples e razoavelmente eficaz na integração vertical. Contudo, devido, quer à ausência de adequação destes sistemas para o problema em causa, quer à proliferação de equipamentos de controlo com características muito diversas, a utilização desta tecnologia acabou por resultar em soluções bastante limitadas.

Nos finais dos anos 90, devido às crescentes exigências de integração com aplicações de nível intermédio e superior, nomeadamente o ERP (Enterprise Resource Planning) e o MES (Manufacturing Execution System), foram desenvolvidas um conjunto de tecnologias de *software* baseadas em plataformas de objectos distribuídos, que disponibilizavam uma

infraestrutura ao nível dos serviços de comunicações, permitindo assim desenvolver de forma eficaz os conceitos de integração vertical e horizontal. São exemplos destas tecnologias o CORBA (Common Object Request Broker Architecture), com uma gama alargada de domínios de aplicação, e o OPC (Object linking and embedding for Process Control), que foi especialmente desenvolvido para satisfazer os requisitos no domínio das aplicações industriais. Este processo apresenta actualmente uma grande dinâmica, com destaque para o desenvolvimento de *standards* com base em arquitecturas de objectos distribuídos especialmente vocacionados para as necessidades dos ambientes industriais: IEC 61499 (Function Blocks for Industrial-Process Measurement and Control Systems) e o IEC 61804 (Function Blocks for Process Control). Como resultado deste trabalho, as arquitecturas de comunicação mais recentes já incorporam muitas destas funcionalidades, das quais se destacam: o CIP (Common Industrial Protocol), o IDA (Interface for Distributed Automation), o HSE *fieldbus* (High Speed Ethernet) e o PROFINET.

Entre os finais dos anos 90 e o início da corrente década verificou-se um fenómeno de migração de tecnologias de uso geral para a área das comunicações industriais. O caso mais paradigmático deu-se com a utilização da rede Ethernet em ambientes industriais (IE - Industrial Ethernet). Este processo teve um profundo impacto na estrutura das comunicações industriais, afectando todos os níveis de controlo. Esta migração deveu-se a vários factores, tais como: a existência de soluções de *hardware* de baixo custo e de elevado desempenho, bem como de protocolos de comunicação abertos e a disponibilização de plataformas de *software* para o desenvolvimento integrado de aplicações distribuídas.

A etapa mais recente desta evolução está centrada na utilização das tecnologias desenvolvidas para Web, tais como UDP/TCP/IP (User Datagram Protocol / Transmission Control Protocol / Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), XML (eXtensible Markup Language), Proxys, Java, ou Jini, para o desenvolvimento de aplicações industriais. A utilização destas tecnologias, para além de estarem largamente difundidas e do seu custo reduzido, vai permitir obter níveis de integração superiores nomeadamente ao nível dos domínios de aplicação externos ao ambiente industrial [11].

Associado ainda a este processo de migração de tecnologias emergentes para as redes industriais, é de salientar a crescente tendência para a utilização de redes de comunicações sem fios (como o IEEE 802.11 ou o IEEE 802.15) em ambientes industriais [9], [10].

2.3 O Modelo de Referência OSI

Convém agora, fazer uma descrição do modelo OSI, uma vez que os protocolos de comunicações industriais a seguir mencionados têm como referência esse modelo.

Num ambiente onde existem equipamentos provenientes de diferentes fabricantes a integração implica a definição de protocolos de comunicação normalizados. A ISO (International Organization for Standardization) definiu o modelo de referência OSI com o objectivo de promover o aparecimento de normas na área das comunicações entre computadores, equivalente ao que na altura se verificava já para as comunicações telefónicas, definidas no âmbito da CCITT (Commité Consultatif International de Telegraphique et Telephonique) [12]. O termo "sistema de arquitectura aberta" indica que se um sistema estiver conforme com o modelo OSI então está aberto a comunicar com qualquer outro que obedeça às mesmas normas. É de salientar que o modelo de referência OSI não especifica por si as normas de comunicação. O seu propósito é apenas fornecer uma arquitectura que sirva de base ao desenvolvimento de normas para sistemas de comunicação.

O modelo de referência OSI define 7 camadas, conforme se indica na figura 2.5.

Figura 2.5 - O modelo de referência OSI

A hierarquia dos níveis vai subindo, desde o nível de maior especificidade até ao mais alto, que é o nível mais genérico.

Os três primeiros níveis fornecem um serviço de rede, ou seja, tratam do transporte da informação. O nível físico trata do meio físico para a transmissão de *bits* de informação, o nível lógico organiza os *bits* de uma forma ordenada em blocos (tramas) e assegura que eles são transmitidos e recebidos de uma forma correcta, enquanto o nível de rede assegura que os pacotes chegam ao seu destino final.

Enquanto o serviço de rede fornecido pelos três níveis inferiores é adequado para transportar informação, algumas aplicações podem ter especificações que as redes não fornecem, como por exemplo uma taxa de erros baixa, um elevado nível de segurança, ou a necessidade de manter uma sequência de pacotes que façam uma mensagem completa. São estes os serviços que o nível de transporte fornece aos níveis superiores.

Os níveis acima do nível de transporte não tratam de mecanismos de transmissão de informação. Esse é o trabalho dos quatro níveis inferiores. No entanto, a informação necessita de ser sincronizada e tratada para que as aplicações entendam. O nível de sessão fornece o serviço de gestão da comunicação entre aplicações.

Outro ponto importante é o formato em que a informação é trocada. Os dois sistemas que estão a comunicar podem ter maneiras diferentes de representar os dados. O nível de apresentação preenche o requisito de identificar e estabelecer uma sintaxe comum, que será utilizada pelos dois sistemas.

O nível mais alto é o nível de aplicação, que constitui a *interface* entre as aplicações propriamente ditas e o sistema de comunicações.

Tendo sido feita uma introdução do modelo, a seguir é feita uma abordagem mais detalhada, especificando, em cada nível: os seus objectivos, os serviços oferecidos ao nível imediatamente superior e as suas funções.

2.3.1 O Nível Físico

O nível físico é responsável por uma transmissão transparente da informação através do meio físico. As funções do nível físico são inteiramente independentes do meio físico em uso, seja este constituído por fio de cobre, cabo coaxial ou fibra óptica. O tipo de meio físico utilizado é completamente escondido ao nível lógico pelo nível físico.

As definições do nível físico podem ser agrupadas da seguinte forma:

- Mecânicas: definem o tipo de conector, as dimensões físicas, as posições dos

pinos, etc;

- Eléctricas: definem as características eléctricas, como por exemplo: níveis eléctricos, impedância, etc;
- Funcionais: definem qual o significado dos níveis eléctricos em determinados pinos do conector;
- Procedimentais: definem as regras (procedimentos) a aplicar às várias funções e também qual a sequência em que determinados eventos podem ocorrer.

Serviços Fornecidos ao Nível Lógico

O nível físico fornece os seguintes serviços ao nível lógico:

- Ligações físicas: o fornecimento de uma transmissão de *bits* perfeitamente transparente entre entidades lógicas. A ligação física estabelece um "circuito de informação" entre dois pontos. A ligação física pode ser estabelecida entre dois pontos ou directamente, ou através de um sistema intermédio;
- Tratamento das unidades de informação: este serviço compreende a transmissão de um *bit* em transmissão série, ou de n *bits* em transmissão paralela. A ligação física pode ser *full-duplex* (a informação é feita nos dois sentidos simultaneamente), *half-duplex* (a informação é feita nos dois sentidos mas alternadamente), ou ainda *simplex* (a informação só é feita num sentido);
- Ligação entre pontos: a ligação entre pontos pode ser ponto-a-ponto ou multiponto;
- Sequenciamento: o nível físico coloca os *bits* no meio físico na mesma ordem que lhe foram fornecidos pelo nível lógico
- Identificação de circuito: o nível físico fornece identificadores que definem univocamente a ligação entre dois sistemas. O nível físico fornece identificadores da ligação entre pontos, que podem ser utilizados pelo nível lógico;
- Recuperação de falhas: o nível lógico é notificado de problemas detectados pelo nível físico;
- Parâmetros fornecidos ao nível lógico: são fornecidos parâmetros ao nível lógico, tais como: taxas de erro, taxas de transmissão, disponibilidade de serviço e atrasos.

Funções do Nível Físico

As seguintes funções são executadas pelo nível físico:

- Estabelecimento e libertação das ligações entre entidades do nível lógico;
- Transmissão de sequências de *bits*: estas podem ser síncronas ou assíncronas;
- Gestão: os protocolos do nível físico tratam de alguns aspectos relacionados com a gestão das actividades deste nível.

2.3.2 O Nível Lógico

O nível lógico isola os níveis superiores das características do meio de transmissão e fornece uma ligação sem erros e de confiança. O nível lógico é estabelecido sobre uma ou mais redes físicas e liga duas identidades em sistemas adjacentes. As ligações lógicas são ponto-a-ponto.

Dentro do nível lógico as sequências de *bits* do nível físico são organizadas em blocos de informação denominados tramas. São funções do nível lógico a sincronização dos *bits* dentro de uma trama, a detecção e correcção de erro (através da retransmissão de pacotes) e ainda o controlo de fluxo (dependendo do estado do sistema de recepção, liga ou desliga a transmissão de pacotes).

Serviços Fornecidos ao Nível de Rede

Os seguintes serviços são fornecidos pelo nível lógico:

- Ligação lógica: o estabelecimento de uma ou mais ligações entre duas entidades;
- Unidades de informação do nível lógico: estas entidades teóricas são mapeadas numa base de uma para uma em unidades do protocolo em uso. Na prática, estas são as tramas transmitidas numa ligação lógica;
- Identificadores lógicos: se requerido pelo nível físico, o nível lógico pode fornecer identificadores dos pontos da ligação lógica;
- Sequenciamento: manutenção da sequência correcta de pacotes;
- Detecção de erros: se for detectado um erro não recuperável pelo nível lógico, então o nível físico será notificado;
- Controlo de Fluxo: o nível de rede pode controlar dinamicamente a taxa a que pode receber os pacotes;
- Parâmetros da qualidade do serviço: estes parâmetros são opcionais e incluem

tempos médios entre erros detectados mas irrecuperáveis, taxa de erro residual, disponibilidade do serviço e débito.

Funções do Nível Lógico

As seguintes funções são efectuadas no nível lógico:

- Estabelecimento e libertação das ligações do nível lógico: como foi referido, esta função faz um mapeamento das unidades de informação em unidades do protocolo, em uso numa forma de uma para uma;
- Separação de ligações lógicas: esta função é feita dividindo uma ligação lógica em várias ligações físicas;
- Delimitação e sincronização: esta é essencialmente uma função de empacotamento, que organiza *bits* (unidades do nível físico) em tramas (unidades lógicas);
- Controlo de sequência: mantém a ordem sequencial dos pacotes transmitidos através da ligação lógica;
- Detecção de erros: esta função detecta erros de transmissão, de formato e de operação, que usualmente aparecem devido a deficiências no meio físico;
- Recuperação de erros: esta função tenta recuperar os erros, geralmente através da retransmissão de pacotes;
- Controlo de fluxo: fornece os serviços de controlo de fluxo já descritos;
- Identificação e troca de parâmetros: efectua a identificação de entidades lógicas e controla a troca de parâmetros;
- Controlo da ligação do circuito de dados: esta função fornece o nível de rede com a informação necessária para controlar e manter o circuito de dados ao nível de rede;
- Gestão: os protocolos do nível físico tratam de alguns aspectos da gestão das actividades deste nível.

2.3.3 O Nível de Rede

A função essencial do nível de rede é fornecer uma transmissão de dados perfeitamente transparente de um nível de transporte de um sistema (por exemplo uma aplicação num terminal) a um nível de transporte de outro sistema (por exemplo a aplicação servidora num computador central).

Em redes complexas, entidades comunicantes no nível de transporte não necessitam de estar próximas, mas ligadas através de um ou mais sistemas intermédios. Nestes casos, o nível de rede fornece funções de encaminhamento. Um exemplo pode ser a ligação de uma rede pública de dados com uma rede privada (por exemplo uma rede bancária) e uma rede local. Os endereços de rede são utilizados para identificar as várias entidades comunicantes no nível de transporte ao nível de rede.

Serviços Fornecidos ao Nível de Transporte

Os seguintes serviços são fornecidos pelo nível de rede:

- Endereços de rede: são fornecidos pelo nível de rede e são usados por entidades do nível de transporte, de forma a identificar univocamente outras entidades do nível de transporte;
- Ligações de rede: fornecem os meios de transferir dados entre entidades do nível de transporte;
- Identificadores de Ligações Rede entre sistemas: o nível de rede fornece às entidades do nível de transporte um identificador de ligação associado univocamente com o endereço de rede;
- Unidades de informação do nível de rede: numa ligação de rede o nível de rede fornece, para transmissão, unidades de informação (pacotes de dados). Estas unidades têm um cabeçalho e um final perfeitamente definidos. A integridade da unidade é verificada no nível de rede;
- Parâmetros de qualidade do serviço: estes parâmetros incluem taxa residual de erros, disponibilidade do serviço, habilidade, débito, atraso no tráfego e atraso no estabelecimento de ligações na rede;
- Notificação de erros: erros irrecuperáveis para o nível de rede são participados ao nível de transporte;
- Sequenciamento: o nível de rede pode fazer a entrega de unidades de informação do nível de rede sequencialmente para uma determinada ligação de rede;
- Controlo de fluxo: a entidade de transporte que está a receber pode fazer com que o Serviço de Rede pare de enviar mais unidades de informação. Este controlo de fluxo pode ou não ser enviado ao outro extremo da ligação;
- Libertação: a entidade de transporte pode pedir a libertação da ligação.

Funções do Nível de Rede

As funções de nível de rede fornecem uma grande variedade de configurações, desde ligações ponto-a-ponto a ligações mais complexas, com uma combinação de várias sub-redes. As seguintes funções são efectuadas:

- Encaminhamento e repetição: as ligações da rede são fornecidas por entidades nos sistemas finais, mas podem ser envolvidas entidades em sistemas intermédios que façam repetição. As funções de encaminhamento determinam um caminho definido entre dois endereços;
- Ligações de rede: esta função fornece ligações entre entidades do nível de transporte, fazendo uso de ligações fornecidas pelo nível lógico;
- Multiplexação de ligações de rede: esta função é usada para multiplexar ligações de rede em ligações lógicas;
- Segmentação e empacotamento: o nível de rede pode segmentar e/ou formar blocos que constituem unidades de informação do nível de rede, para facilitar o transporte;
- Funções de detecção de erros: são utilizadas para verificar se a qualidade dos serviços fornecidos numa rede é mantida. Quando há detecção de erros no nível de rede o nível lógico é notificado. As funções de recuperação de erros dependem da qualidade do Serviço de Rede fornecido;
- Sequenciamento: prevê a entrega sequencial de unidades de informação do Serviço de Rede numa determinada ligação;
- Controlo de fluxo;
- Selecção de serviços: esta função permite que sejam seleccionadas as mesmas funções nos dois sistemas, mesmo quando a ligação se faz entre vários subsistemas.

2.3.4 O Nível de Transporte

O papel do nível de transporte é complementar a rede que está por baixo, de forma a assegurar a qualidade dos serviços requeridos que estão acessíveis ao utilizador.

As funções do nível de transporte estão focalizadas em optimização de custos, controlo de erros, controlo de fluxos, sequenciamento e multiplexagem. O nível de transporte também verifica a existência de duplicados e perdas de informação. Se a ligação de rede for quebrada temporariamente, a ligação de transporte pode ser mantida até que a ligação seja restaurada.

Os protocolos do nível de Transporte são definidos para aceitar uma grande variedade de redes, com várias qualidades de serviços. São cinco as classes de Serviços de Transporte disponíveis:

- A classe 0 é a classe mais simples, sem melhoramentos nos Serviços de Rede;
- A classe 1 adiciona recuperação de erros para redes sujeitas a uma grande frequência de interrupções;
- A classe 2 tem as funções da classe 0 mais multiplexagem;
- A classe 3 tem as funções da classe 1 mais multiplexagem;
- A classe 4 adiciona funções de detecção de erros e de dados fora de sequência.

Serviços Fornecidos ao Nível de Sessão

Os seguintes serviços são fornecidos pelo nível de transporte:

- Estabelecimento de ligações de transporte: as ligações de transporte são estabelecidas entre identidades do nível de sessão e são identificadas pelo endereço de transporte. A qualidade do serviço é negociada entre as entidades do nível de sessão e o serviço de transporte;
- Transferência de dados: fornece a transferência de dados, de acordo com a qualidade de serviço que foi negociada;
- Libertação da ligação de transporte: fornece meios para que qualquer entidade da camada de sessão dos sistemas possa libertar a ligação de transporte.

Funções do Nível de Transporte

As operações no nível de transporte são:

1 Fase de Iniciação

Durante esta fase são efectuadas as seguintes funções:

- Obtenção de uma ligação à rede que corresponda aos requisitos em termos de custos e qualidade de serviço.
- Decisão de multiplexagem ou divisão.
- Estabelecer as unidades de informação do protocolo de transporte óptimas.
- Selecção das funções que devem estar operacionais durante a transferência de dados.
- Mapeamento dos endereços de transporte em endereços de rede.

- Fornecimento de identidade aos endereços de transporte.
- Transferência dos dados.

2 Fase de Transferência

Durante esta fase é executada a transmissão de unidades de informação do protocolo de transporte. Os seguintes serviços podem ser usados ou não, dependendo da classe de serviço seleccionada:

- Sequenciamento;
- Empacotamento;
- Segmentação;
- Multiplexagem ou divisão;
- Controlo de fluxo;
- Detecção e recuperação de erros;
- Transferência dos dados enviados;
- Delimitação das unidades de informação do serviço de transporte;
- Identificação das ligações de transporte.

3 Fase de Libertação

Esta fase inclui as seguintes funções:

- Notificação das razões da libertação.
- Identificação da ligação de transporte libertada.
- Transferência de dados.

2.3.5 O Nível de Sessão

Os requisitos para o nível de sessão reflectem a observação da utilização dos sistemas, pela maior parte dos utilizadores, em picos de actividade que podem ser chamados de sessões. Durante a sessão, o utilizador e o sistema iniciam um diálogo. A primeira função do nível de sessão é estabelecer, manter e gerir este diálogo.

As ligações da camada de Sessão são mapeadas em ligações da camada de transporte numa razão de um para um. Não existe multiplexagem neste nível, mas é possível que várias ligações de sessão usem a mesma ligação de transporte sequencialmente. Simultaneamente, uma ligação de sessão pode usar mais que uma ligação de transporte. Se a ligação de transporte se quebrar, devido a problemas nas camadas inferiores da rede, é possível estabelecer uma nova ligação de transporte sem a intervenção do utilizador ou

mesmo chegar ao seu conhecimento a quebra. Neste caso é o nível de sessão que é o responsável pela ressincronização do diálogo entre os dois sistemas.

Serviços Fornecidos ao Nível de Apresentação

Os seguintes serviços são fornecidos pelo nível de sessão:

- Estabelecimento da ligação entre níveis de sessão: permite que duas entidades do nível de apresentação possam estabelecer uma ligação de sessão entre elas;
- Libertação de ligação: permite que entidades do nível de apresentação possam libertar uma ligação do nível de sessão de uma forma ordeira e sem perda de informação;
- Transferência de dados: permite que uma entidade emissora do nível de apresentação possa transferir uma unidade de informação do nível de sessão a uma entidade receptora do nível de apresentação;
- Serviço de Quarentena: permite à entidade emissora solicitar que algumas unidades de informação, enviadas por uma conexão do nível de sessão, não devam ser enviadas à entidade receptora do nível de apresentação, até ordem contrária enviada pelo emissor;
- Gestão de Interacção: permite que entidades do nível de apresentação comandem explicitamente quem vai controlar certas funções de controlo. São possíveis os seguintes tipos de interacção: dois sentidos simultaneamente, dois sentidos alternadamente, um sentido;
- Sincronização de ligação: este serviço permite que entidades do nível de apresentação definam e identifiquem pontos de sincronização que obriguem uma ligação do nível de sessão a permanecer num determinado estado (*reset*) e que definam qual o ponto de ressincronização;
- Situações excepcionais: faz a notificação ao nível superior de quaisquer situações não englobadas pelos serviços deste nível.

Funções do Nível de Sessão

A maior parte das funções necessárias neste nível estão implícitas aos serviços deste nível:

- Mapeamento das ligações de sessão às ligações de transporte;
- Controlo do fluxo do nível de sessão: o nível de sessão não possui controlo de fluxo. Para evitar aumentar as funções do nível de sessão este controlo é feito no nível de

transporte;

- Recuperação de ligações quebradas: no caso de quebra de ligação do nível de transporte o nível de sessão pode ter as funções necessárias para restabelecer uma nova ligação, de forma a continuar a sessão;
- Libertação da ligação de Sessão: permite que se acabe e liberte a ligação sem perda de informação.

2.3.6 O Nível de Apresentação

Este nível é responsável por assegurar que a informação é apresentada ao utilizador de uma forma útil (através do nível de aplicação). O nível de apresentação só trata da sintaxe da informação (a forma como é representada a informação) e não com a sua semântica (significado da informação).

Serviços Fornecidos ao Nível de Aplicação

Os seguintes serviços são fornecidos pelo nível de apresentação:

- Transformação da Sintaxe: trata dos códigos e do conjunto de caracteres a usar (por exemplo o código ASCII), bem como da apresentação da informação (por exemplo a visualização da informação num monitor);
- Selecção da Sintaxe.

Funções do Nível de Apresentação

As funções do nível de apresentação são:

- Negociação e Renegociação da Sintaxe;
- Transformação da Sintaxe;
- Gestão da passagem de serviços dos Níveis Sessão e Aplicação.

2.3.7 O Nível de Aplicação

O nível de apresentação constitui o *interface* entre as aplicações propriamente ditas e o sistema de comunicação. As aplicações trocam informação entre si, utilizando entidades e protocolos do nível de aplicação e serviços do nível de apresentação.

Serviços Fornecidos às Aplicações

Além da transferência da informação, estes serviços podem incluir:

- Identificação dos vários intervenientes da comunicação através do nome, endereço e descrição;
- Determinação da disponibilidade dos intervenientes;
- Verificação e validação dos intervenientes;
- Determinação dos recursos necessários;
- Determinação da qualidade de serviço mínima;
- Sincronização de aplicações;
- Selecção da forma de diálogo;
- Entendimento na responsabilidade na recuperação de erros;
- Acordo na forma de controlo da integridade da informação;
- Identificação de limitações na sintaxe da informação.

Funções do Nível de Aplicação

O nível de aplicação contém todas as funções exigidas pela comunicação entre sistemas abertos, mas que não são fornecidas pelos níveis inferiores. As comunicações entre aplicações são efectuadas através de entidades do nível de aplicação. Estas entidades representam conjuntos de capacidades de comunicação OSI e estão divididas em elementos específicos implementados pelo utilizador e elementos pertencentes aos serviços do nível de aplicação, sendo estes últimos denominados por ASE (Application Service Element).

Um exemplo de um serviço do tipo ASE é o MMS (Manufacturing Message Specification), que é uma norma internacional do nível de aplicação vocacionada para o ambiente industrial.

2.4 A Arquitectura das Comunicações Industriais

Ao nível dos sistemas de controlo a integração implica a necessidade de cooperação e interacção entre os vários subsistemas incluídos no mesmo sistema. Isto significa transferência, armazenamento e processamento de informação em ambientes com características heterogéneas, o que por sua vez obriga à necessidade de dispor de uma infra-estrutura de comunicações adequada. As redes locais industriais, não sendo a solução para este problema, são contudo uma parte integrante e essencial dessa solução.

Os fluxos de informação existentes num ambiente industrial possuem características de tal forma distintas que não é possível dispor de uma única rede capaz de satisfazer todas

as necessidades de comunicação. Desta forma, a alternativa é dispor de um conjunto de redes que no seu conjunto sejam capazes de satisfazer a totalidade dessas necessidades. Num sistema automatizado as actividades relacionadas com o controlo do processo industrial podem ser estruturadas num modelo hierárquico caracterizado por fluxos de informação verticais entre entidades de níveis hierárquicos adjacentes e por fluxos de informação horizontais entre entidades do mesmo nível hierárquico. Como estas actividades estão intimamente associadas à estrutura de comunicações que lhes serve de suporte, surge de forma natural a adopção de um modelo hierárquico para a arquitectura de comunicações (Figura 2.6) [5].

Figura 2.6 - Relação entre os níveis de controlo e a arquitectura de comunicações

Embora os modelos hierárquicos para a estrutura de controlo possam variar em número de níveis, tipicamente entre o 4 e o 6, ao nível da arquitectura de comunicações é usual identificar três níveis distintos: fábrica, célula e campo. Para cada um destes níveis foram desenvolvidas várias soluções, cada uma possuindo diferentes objectivos, protocolos, capacidades e complexidade:

- Fábrica - Cobrem as necessidades dos níveis superiores. As principais actividades encontradas a este nível são o planeamento da produção, de processos e de materiais e as áreas de engenharia financeira e comercial. O fluxo de informações descendente centra-se essencialmente nas ordens de fabrico e nas informações associadas ao seu escalonamento. No sentido ascendente circulam informações relativas ao estado das ordens de fabrico, à qualidade do processo produtivo e a pedidos de aquisição de materiais e/ou recursos. Este nível é caracterizado por um elevado fluxo de informação horizontal entre e dentro dos vários subsistemas existentes sem requisitos temporais críticos.

- Célula - Cobrem as necessidades dos níveis intermédios. Uma célula agrupa um conjunto de equipamentos que cooperam para a execução de uma determinada tarefa. As principais actividades encontradas a este nível são o escalonamento, o sequenciamento e a execução de tarefas. Outras actividades também executadas têm a ver com a compilação da informação relativa à qualidade da produção e ao desempenho dos equipamentos que constituem a célula. A informação que circula do nível célula para os níveis descendentes inclui ordens de execução de operações ou programas de controlo, no caso de equipamentos programáveis. Em sentido ascendente a informação disponibilizada diz respeito à evolução das operações executadas e aos resultados dessas mesmas operações. Este nível é caracterizado por fluxos de informação de volume intermédio e com requisitos temporais exigentes, que em muitos casos podem ser críticos.
- Campo - Cobrem as necessidades dos níveis mais baixos. As principais actividades encontradas a este nível estão relacionadas com o controlo directo do processo industrial, nomeadamente a execução de algoritmos de controlo, por equipamentos que actuam fisicamente sobre os materiais ou produtos a operar. A *interface* com o processo é realizada por intermédio de sensores e actuadores, muitos deles dotados de capacidades de processamento complexas (*smart sensors*). Este nível é caracterizado por fluxos de informação de pequeno volume e com requisitos temporais críticos.

2.5 Redes de Campo

As redes de campo foram inicialmente desenvolvidas com o objectivo de satisfazer os requisitos de comunicação dos níveis mais baixos das arquitecturas de controlo industriais. Entre estes destacam-se, pela sua importância, os seguintes [14], [15]:

- Capacidade de transferir pequenos volumes de informação de forma eficiente;
- suportar tráfego periódico (por exemplo amostragem de dados) e aperiódico (por exemplo eventos) com tempos de resposta majorados. Existem assim requisitos de tempo real associados às comunicações;
- capacidade de operar em ambientes industriais típicos, sujeitos a interferências electromagnéticas, vibrações, corrosão, poeiras, humidade, etc;
- garantir um nível adequado de confiança no funcionamento, nomeadamente no que diz respeito à fiabilidade, disponibilidade e segurança e
- baixo custo de aquisição, instalação, operação e manutenção.

De forma a satisfazer estes requisitos foi adoptada uma *stack* de comunicação organizada de acordo com o modelo OSI, mas compactada em 3 níveis: físico, ligação de dados e aplicação. O nível de aplicação incorpora algumas funcionalidades definidas nos restantes níveis não utilizados neste modelo.

Para cada um dos níveis podem ser definidos múltiplos serviços e protocolos de comunicação com características muito diversas. A escolha destes elementos resulta essencialmente dos objectivos originais definidos pelos fabricantes das redes de campo, que de uma forma sucinta podem ser expressos segundo duas perspectivas [15]:

- A rede de campo é considerada apenas como uma forma de simplificar as ligações físicas entre os vários dispositivos ou
- a rede de campo é considerada a coluna vertebral (*backbone*) de um sistema distribuído e de tempo-real.

A diferença entre estas duas perspectivas foi uma das razões que levaram à proliferação de soluções para as redes de campo. Outras razões estão relacionadas com a ausência de um *standard* internacional único e genérico.

2.5.1 Standardização das Redes de Campo

Já no início dos anos 70 foram instaladas e utilizadas as primeiras redes de campo. No entanto, o trabalho de standardização só teve início em meados dos anos 80. A ideia básica de um *standard* é estabelecer uma especificação de uma forma muito rígida e formal, excluindo a possibilidade de pequenas alterações. Isto dá uma certa noção de confiabilidade e estabilidade da especificação, que por sua vez assegura a confiança dos utilizadores e consequentemente uma boa posição no mercado. Além disso, em muitos países os *standard*s têm uma posição *legally binding*, o que significa que quando um *standard* pode ser aplicado é obrigatório aplicá-lo. Isto implica que um sistema standardizado ganha uma posição competitiva em relação aos rivais não standardizados. Não é então de admirar que fosse iniciada uma corrida para a standardização.

A standardização internacional das redes de campo foi sempre difícil. Teve o seu início em 1985 e, depois de uns anos entusiásticos de desenvolvimento, a procura de um único *standard* foi ficando enredada numa rede de políticas de companhias e de interesses de *marketing* [7].

Na segunda parte dos anos 80, no início dos trabalhos da comissão técnica TC 65C do IEC (International Electrotechnical Commission) o desenvolvimento dos sistemas

fieldbus foi basicamente um projecto europeu, levado a cabo, não só por investigadores com um *background* académico, mas também por muitos proprietários. Os resultados mais promissores foram o francês FIP e o alemão PROFIBUS. Ambos foram standardizados a nível nacional e posteriormente propostos ao IEC para standardização internacional. No entanto, as abordagens dos dois sistemas eram completamente diferentes. O PROFIBUS baseava-se no controlo distribuído e a sua forma original suportava uma comunicação vertical orientada ao objecto, de acordo com o modelo cliente-servidor, no espírito da especificação MAP/MMS. Por outro lado, o FIP foi desenvolvido segundo um esquema de controlo centralizado mas capaz de suportar comunicação em tempo real, de acordo com o novo modelo para comunicação horizontal produtor-consumidor ou *publisher-subscriver*.

Como eram muito diferentes, os dois sistemas satisfaziam os requisitos de áreas de aplicação diferentes. Evidentemente, um *fieldbus* universal tinha de combinar os benefícios dos dois, pelo que um grupo de peritos apresentou uma nova proposta, o WorldFIP, que é uma extensão do FIP ao qual foi acrescentada a funcionalidade do modelo cliente-servidor. Por outro lado, o ISP (Interoperable System Project) tentou demonstrar que o PROFIBUS poderia ser melhorado com a introdução do modelo de comunicação *publisher-subscriber*. No entanto o ISP foi abandonado em 1994 por razões estratégicas [7].

Ao mesmo tempo, o papel de líder nos trabalhos de standardização ao nível do IEC foi sendo tomado, não pelos europeus, mas pelo comité SP50 do ISA (International Society of Automation), que foi muito mais eficiente no fim dos anos 80 e teve uma influência importante na estrutura de camadas do *standard* actual. No entanto, até meados dos anos 90 o comité do IEC não tinha produzido nenhum resultado substancial durante mais de 8 anos. A única excepção foi a definição da camada física, que foi adoptada como um *standard* IEC 61158-2 em 1993.

Em 1995, depois de longos anos de disputas entre investigadores alemães e franceses, com vista a combinar as abordagens FIP e PROFIBUS, várias companhias, basicamente americanas, decidiram não continuar a testemunhar as infindáveis discussões. Com o fim do projecto ISP, iniciaram a definição de uma nova rede de campo optimizada para a indústria de processos: o FF (Fieldbus Foundation). Este trabalho foi feito à parte dos comités IEC, dentro do ISA, e por algum tempo o trabalho no IEC pareceu posto de parte.

A 15 de junho de 1999 o comité de acção do IEC decidiu tomar um novo rumo e um mês depois, a 16 de Junho, os representantes das principais partes interessadas na

standardização *fieldbus* (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, PROFIBUS User Organization e Siemens) assinaram um “Memorando de Entendimento”, com o objectivo de pôr um ponto final na disputa dos *standards fieldbus*.

Este processo culminou em 2003 com a adopção de uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 (Digital Data Communications for Measurement and Control - Fieldbus for use in Industrial Control Systems) e o IEC 61784 (Digital Data Communications for Measurement and Control - Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems), sendo ambos constituídos por um conjunto de perfis de comunicação, aos quais acabaram por corresponder as soluções comerciais mais importantes existentes à data da sua publicação (Tabela 2.1) [7].

Tabela 2.1 - Perfis e protocolos de acordo com o IEC 61784 e o IEC 61158

IEC 61784 Perfil	IEC 61158 Protocolos-camadas			Standard CENELEC	Nome comercial
	Física	Ligação de dados	Aplicação		
CPF-1/1	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H1)
CPF-1/2	Ethernet	TCP/UDP/IP	Tipo 5	-	Foundation Fieldbus (HSE)
CPF-1/3	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H2)
CPF-2/1	Tipo 2	Tipo 2	Tipo 2	EN-50170-A3	ControlNet
CPF-2/2	Ethernet	TCP/UDP/IP	Tipo 2	-	Ethernet/IP
CPF-3/1	Tipo 3	Tipo 3	Tipo 3	EN-50254-3	PROFIBUS-DP
CPF-3/2	Tipo 1	Tipo 3	Tipo 3	EN-50170-A2	PROFIBUS-PA
CPF-3/3	Ethernet	TCP/UDP/IP	Tipo 10	-	PROFINET
CPF-4/1	Tipo 3	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-485
CPF-4/1	Tipo 1	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-232
CPF-5/1	Ethernet	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS)
CPF-5/2	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS, subMMS)
CPF-5/3	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS)
CPF-6/1	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS
CPF-6/2	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS TCP/IP
CPF-6/3	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS Subset
CPF-7/1	Tipo 1	Tipo 6	-	-	Swiftnet transport
CPF-7/2	Tipo 1	Tipo 6	Tipo 6	-	Swiftnet full stack

Como se pode verificar pela tabela, sistemas *fieldbus* simples, como o CAN e o AS-*Interface*, não foram incluídos nesta norma. Estes estão incluídos num *standard* específico para este tipo de sistemas, o IEC 62026 (Low-voltage switchgear and controlgear - Controller-Device Interfaces), publicado em Junho de 2007.

À medida que o processo de standardização foi estabilizando, o desenvolvimento focou-se na definição de uma quarta camada, denominada camada de utilizador. O seu objectivo é disponibilizar ao utilizador uma abordagem integrada no desenvolvimento das aplicações, nomeadamente através da definição de blocos funcionais, linguagens de descrição dos dispositivos, interoperabilidade e métricas da qualidade de serviço.

Quanto ao seu posicionamento em relação aos níveis de controlo das aplicações industriais, as redes de campo sofreram uma evolução, passando também a ser utilizadas presentemente como redes de célula. A própria terminologia tem evoluído, através da definição de um conjunto de subcategorias para as redes de campo (Figura 2.7) [5]. Neste sentido, o termo original *fieldbus* tem sido utilizado para designar as redes de campo que estão mais próximas do conceito de rede de célula (ex. PROFIBUS-DP, WorldFIP) e o termo *sensorbus* para designar as redes mais básicas e mais próximas do conceito original de rede de campo (ex. AS-Interface, INTERBUS-S), enquanto o termo *devicebus* é utilizado para designar as que estão num plano de actuação intermédio (ex. DeviceNet, FF-H1). Contudo, e por uma questão de simplificação de linguagem, utiliza-se nesta dissertação apenas os termos rede de campo ou *fieldbus* para representar todas as subcategorias acima definidas.

Figura 2.7 - Categorias das redes de campo

2.6 Ethernet em Tempo Real

Ao mesmo tempo que decorria a standardização *fieldbus*, no mundo administrativo eram implementadas redes baseadas na Ethernet e no TCP/IP. Os custos associados a estas

infra-estruturas têm vindo continuamente a baixar e tornou-se possível ligar quase tudo, em qualquer lado do mundo, com a ajuda da tecnologia da Internet. No entanto, no campo da automação, ainda eram utilizados *fieldbuses* dedicados, a única barreira para aceder a componentes no chão de fábrica via Internet.

Depois de mais de 1 década de experiência com aplicações de *fieldbuses* a indústria começou a desenvolver e a adoptar soluções RTE. Os *standard*s propostos pelo IEC tentam traçar uma linha de orientação e critérios de selecção baseados em indicadores reconhecidos.

A adopção da tecnologia Ethernet na comunicação industrial pressupõe capacidades Internet, como por exemplo *interfaces* com o utilizador remotos, via Web. No entanto, é uma solução inaceitável se a adopção da tecnologia Ethernet causa perda de características necessárias no chão de fábrica, tais como [18]:

- Comunicação determinística;
- acções sincronizadas entre componentes e
- troca de pequenos pacotes de dados eficiente e frequente.

Um requisito implícito e essencial é a capacidade de comunicação Ethernet no nível de escritório ser totalmente absorvida, de modo que o *software* de comunicação envolvido possa ser utilizado. Isto resulta nos seguintes requisitos:

- Suporte de migração da Ethernet do nível do escritório para RTE e
- uso de componentes *standard* (*bridges*, controladores Ethernet e *stack*s de protocolo).

Para se obter a necessária alta qualidade de transmissão de dados, com *jitter* limitado e com perturbações devidas ao tráfego de dados TCP/IP limitadas é necessário desenvolver novos componentes de rede.

Resumindo, a RTE é uma especificação *fieldbus* que utiliza a Ethernet nos dois níveis mais baixos.

2.6.1 Standardização RTE

O *standard* Ethernet não atinge os requisitos do RTE. Existem diferentes propostas na comunidade de investigação para a modificação da tecnologia Ethernet. O mercado também adoptou soluções técnicas adicionais. A seguir são apresentadas as soluções RTE propostas para standardização.

As *interfaces* de comunicação estão estruturadas em diferentes níveis. Na figura 2.8 estão representadas as estruturas possíveis de um protocolo de comunicação RTE [18]. Comum a todas as redes Ethernet é a infraestrutura de cablagem universal.

As aplicações *non real time* utilizam os protocolos Ethernet, tal como definido no ISO 8802-3, e o protocolo TCP/UDP/IP. Utilizam ainda protocolos típicos da Internet, tal como o HTTP ou o FTP.

Figura 2.8 - Estruturas possíveis de uma RTE

Para uma solução RTE existem três diferentes abordagens:

- Na primeira mantêm-se os protocolos TCP/UDP/IP e a modificação que garante o tempo real é feita no nível mais alto. É a solução *on top of* TCP/IP.
- Na segunda não são utilizados os protocolos TCP/UDP/IP e a funcionalidade Ethernet é acedida directamente. É a solução *on top of Ethernet*.
- Na terceira abordagem o mecanismo Ethernet e a própria infraestrutura são modificados de forma a obter uma *performance* em tempo real. É a *Modified Ethernet*.

Na secção seguinte são apresentados os protocolos RTE que existem no mercado.

2.6.2 Protocolos RTE

O IEC 61784-2 (Industrial Communication Networks - Profiles – Part 2: Additional Fieldbus Profiles for Real time Networks based on ISO/IEC 8802-3) é o documento *standard* que especifica pelo menos dez diferentes soluções técnicas para RTE, sendo muitas delas incompatíveis [18] (Tabela 2.2). Alguns dos protocolos propostos apenas

estão definidos, não existindo ainda produtos no mercado. No caso de outros protocolos já existem produtos e aplicações.

Tabela 2.2 - Perfis RTE definidos no IEC 61784

Perfil IEC 61784	**Nomes comerciais**	***Ethertypes***
CPF-2	ControlNet (Ethernet/IP)	(0x0800 IP)
CPF-3	PROFIBUS/PROFINET	0x8892
CPF-4	P-NET	(0x0800 IP)
CPF-10	Vnet/IP	(0x0800 IP)
CPF-11	*TCnet* (Time Critical control network)	0x888B
CPF-12	EtherCAT	0x88A4
CPF-13	EPL (Ethernet PowerLink)	0x88AB
CPF-14	EPA (Ethernet for Plant Automation)	0x88BC
CPF-15	MODBUS – RTPS (Real Time Publisher Subscriber).	(0x0800 IP)
CPF-16	SERCOS (SErial Real time COmmunication System Interface)	0x88CD

Protocolos *on top of* TCP/IP

Algumas soluções RTE utilizam a *stack* do protocolo TCP/UDP/IP sem modificações. Com esta *stack* é possível comunicar de uma forma transparente para além dos limites da rede de campo.

É então possível implementar redes de campo que comuniquem com todos os pontos do mundo, da mesma forma que a tecnologia Internet. No entanto, o manuseamento desta *stack* de protocolo de comunicação requer recursos razoáveis, quer ao nível do processamento, quer ao nível da memória e introduz atrasos não determinísticos na comunicação.

A seguir são apresentadas algumas soluções disponíveis no mercado.

Modbus/TCP

Foi definido pela Schneider Electric e é mantido pela Modbus-IDA. Utiliza o já conhecido Modbus (o *standard* industrial "de facto" desde 1979) sobre uma rede TCP/IP, através da porta 502.

Esta é provavelmente uma das soluções Ethernet mais utilizadas em aplicações industriais e satisfaz os requisitos da classe mais baixa de aplicações, o controlo humano.

É um protocolo muito simples, do tipo *request/reply* (envia uma trama de *request* e recebe uma trama de *reply*). Em adição ao histórico Modbus, este protocolo tem definidas extensões *real time* que utilizam o RTPS. O RTPS prevê dois modelos de comunicação: o

publisher-subscriber, que transfere dados do *publisher* para o *subscriber*, e o CST (Composite State Protocol), que transfere informação de estado de um escritor para um leitor.

Ethernet/IP

Este protocolo foi definido pela Rockwell e é mantido pela ODVA (Open DeviceNet Vendor Association) e pela ControlNet International. Utiliza o CIP, que é comum nas redes Ethernet/IP, ControlNet e DeviceNet.

Este protocolo está incluído no *standard* IEC 61784-1 como CP 2/2 (tipo 2 no IEC 61158) e fornece comunicação *real time* baseada no ISO/IEC 8802-3.

Na Ethernet *full-duplex* não existe a possibilidade de atrasos devidos a colisões. No entanto, as tramas Ethernet podem sofrer atrasos no próprio dispositivo de *switch*, caso a porta de saída esteja ocupada na transmissão de outra trama. Isto pode levar a atrasos não determinísticos, que não são aconselháveis em aplicações em tempo real. Para evitar estes atrasos está definido um mecanismo de prioridades no IEEE 802.3, que permite a atribuição de níveis de prioridade (0 a 7) a tramas Ethernet.

P-NET

O P-NET sobre a especificação IP foi proposto pelo comité nacional dinamarquês e o seu uso destina-se ao ambiente IP. Neste protocolo a comunicação em tempo real P-NET é embebida em pacotes UDP/IP, que tanto podem circular em redes IP como em redes *non* IP.

Uma trama P-NET inclui uma tabela P-Net *route*, que por sua vez é constituída por dois elementos: os endereços da fonte e do destino da própria trama. No caso mais simples de uma rede de campo, estes são os endereços de dois nós da própria rede. Para permitir a comunicação entre dispositivos da rede de campo e dispositivos de uma rede IP os endereços da tabela P-Net *route* terão de ser endereços IP.

De facto, este protocolo apenas especifica a forma como são integradas redes P-NET e redes UDP/IP e não prevê nenhuma medida que assegure um comportamento em tempo real na rede Ethernet.

Vnet/IP

Este protocolo foi desenvolvido pela Yokogama.

Utiliza o TCP/IP para a integração de protocolos Internet, como o HTTP, e de extensões de protocolos *real time*, o RTP (Real Time and reliable datagram Protocol).

Este não é de facto um protocolo RTE, apenas utiliza o protocolo UDP/IP para o transporte do protocolo RTP. Não são tomadas nenhumas medidas especiais que garantam o comportamento determinístico de um protocolo *real time*.

Protocolos *on top of* Ethernet

Estes protocolos RTE não alteram o *hardware* de comunicação Ethernet, mas especificam um tipo de protocolo especial na trama Ethernet, o *Ethertype* (tabela 2.2). Por exemplo, o tipo *standard* para o protocolo IP é *Ethertype*=0X0800. Estes protocolos RTE utilizam, além da *stack* de protocolo IP *standard*, a sua própria *stack* de protocolo identificada com o seu próprio tipo. A tabela 2.2 lista os diferentes valores assignados para as várias soluções.

EPL

Foi definido por Bernecker & Rainer e é mantido pelo grupo de standardização EPL.

Baseia-se num sistema de escalonamento *master-slave* num segmento Ethernet partilhado, o SCNM (Slot Communication Network Management). O *master* é o MN (Managing Node), assegura o acesso em tempo real aos dados cíclicos e apenas permite a comunicação de tramas TCP/IP (*non real time*) em *slots* de tempo reservadas para este tipo de dados. Todos os outros nós são os CNs (Controlled Nodes) e apenas podem enviar dados a pedido do MN.

O ciclo de comunicação de um sistema EPL é composto por quatro períodos: *Start*, *Isochronous*, *Asynchronous* e *Idle* (Figura 2.9) [18]. No período *Start* o MN envia uma trama *multicast* SoC (Start of Cycle), que indica o início do ciclo. No período *Isochronous* o MN envia uma trama *unicast* PReq (Poll Request) para cada um dos CNs e o CN acedido envia uma trama *multicast* PRes (Poll Response). No início do período *Asynchronous* o MN envia uma trama SoA (Start of Asynchronous) e o acesso ao meio é permitido tanto ao MN como a qualquer CN, mas apenas pode ser enviada uma trama ASnd (ASynchronous data). O protocolo tipicamente usado neste período é o UDP/IP. Desta forma a transmissão de dados assíncronos nunca interfere com a transmissão de dados síncronos, o que garante um *timing* preciso na comunicação.

Figura 2.9 - Ciclo de comunicação do EPL

TCnet

É uma proposta da Toshiba. Tal como no EPL, a *interface* TCnet está entre a camada física e a camada de ligação de dados. O acesso MAC (Medium Access Control) típico da Ethernet, o CSMA/CD, é modificado.

O período de transmissão de alta velocidade é composto por um serviço de transmissão de dados cíclico em tempo real (no TCnet utiliza-se a expressão *time critical*) e por um serviço de transmissão assíncrona (no TCnet é denominada como *sporadic*) (Figura 2.10) [18].

Cada período de transmissão de alta velocidade é iniciado com o *broadcast* de uma trama SYN para todos os nós da rede. Depois de receber a trama SYN, o nó 1 inicia a transmissão das suas tramas de dados (DT). Quando termina faz o *broadcast* de uma trama CMP, que indica o fim da sua transmissão. Esta é recebida pelo nó 2, que inicia a transmissão das suas tramas de dados, repetindo-se o processo até ao último nó.

Figura 2.10 - Ciclo de comunicação do TCnet

EPA

O protocolo EPA é uma proposta chinesa.

Este protocolo permite uma comunicação determinística baseada num mecanismo de divisão de tempo dentro da camada MAC. O *macrocycle* (T) é o tempo total para completar um procedimento de transmissão de dados. Esse tempo é dividido em duas fases: a fase para transmissão de mensagens periódicas (Tp) e a fase para transmissão de mensagens aperiódicas (Tn) (Figura 2.11) [18].

A última parte de cada mensagem periódica é um anúncio de mensagem não periódica, que indica se o dispositivo que enviou a mensagem periódica tem ou não uma mensagem não periódica para transmitir. Se tiver, o dispositivo só a poderá enviar na fase Tn.

Figura 2.11 - Ciclo de comunicação do EPA

PROFINET CBA

Foi definido por um conjunto de vários fabricantes, incluindo a Siemens, e é mantido pela PROFIBUS Internacional.

A primeira versão foi baseada no CBA (Component Based Automation) e está incluída no IEC 61784-1 (tipo 10 no IEC 61158).

Para a transmissão de dados sem requisitos de tempo real é utilizada a *stack* TCP/IP e protocolos como o RPC (Remote Procedure Call) e o DCOM (Distributed Component Object Model). Quando é necessária comunicação em tempo real (para ciclos de tempo abaixo dos 100 ms) não é utilizada a *stack* TCP/IP, sendo preferido o protocolo em tempo

real, que é baseado no *Ethertype* 0x8892 e no mecanismo de atribuição de prioridade à trama.

Modified Ethernet

A topologia da cablagem típica da Ethernet é a topologia em estrela: todos os componentes estão ligados a um dispositivo central de *switch*.

Nas aplicações da área da automação, com a introdução do *fieldbus* a topologia em estrela foi substituída por topologias em barramento ou em anel para reduzir os custos na cablagem.

As soluções RTE devem estar preparadas, tanto para as topologias utilizadas no chão de fábrica, como para a topologia da *swicthed Ethernet*. Para isso existem duas soluções: ou a infraestrutura da rede de campo tem um *switch* para cada dispositivo, ou a funcionalidade de *switch* é integrada nos próprios dispositivos da rede de campo.

SERCOS

O SERCOS III é uma extensão RTE do SERCOS, definido pelo *standard* IEC 61491 (Electrical Equipment of Industrial Machines – Serial Data for Real-Time Communication for Controls and Drives), o seu processo de standardização teve início em 2005 e culminou em 2007 com a aprovação do *standard* IEC 61784-2/61158.

No sistema SERCOS existe uma estação *master* e estações *slave*s, cujo número pode variar entre 1 e 254. Todas as estações têm duas portas Ethernet. A topologia da rede pode ser *daisy-chain* ou em anel. Não são permitidos *switches* entre estações e, apenas no caso da topologia *daisy chain*, a porta Ethernet livre do último *slave* pode ser ligada a um *switch*, se for requerida comunicação entre dispositivos via TCP/IP ou UDP/UDP.

No sistema SERCOS III o ciclo de comunicação está dividido em dois períodos, denominados de canais de comunicação: o primeiro é o canal *real time* e o segundo, com menor duração, é o canal *non real time* (Figura 2.12) [18].

O ciclo de comunicação é iniciado pelo *master*, que envia a t*odos os slaves* dois tipos de telegramas *real time*: até 4 MDTs (Master Data Telegrams) e até 4 ATs (Answer Telegrams). Os MDTs contêm informação para sincronização, informação de controlo, dados de serviço do canal e valores de comando. Os ATs são transmitidos pelo *master* como uma trama vazia, mas com campos pré definidos, sendo cada um desses campos destinado a um determinado *slave*. Se um *slave* pretende enviar informação coloca-a no

seu campo e envia o telegrama AT. Quando termina o canal *real time* é iniciado o canal *non real time*, durante o qual podem ser enviados telegramas *non real time*.

Figura 2.12 - Ciclo de comunicação do SERCOS III

ETHERCAT

Este protocolo foi definido pela Beckoff e é mantido pelo grupo de tecnologia Ethercat (ETG). Utiliza as tramas Ethernet e uma topologia em anel especial.

Utiliza um mecanismo de acesso ao meio do tipo *master-slave*, no qual o nó *master* (tipicamente o sistema de controlo) envia tramas *Ethernet standards* ISO/IEC 8802-3 para os nós *slaves*, que por sua vez recebem e enviam dados através dessas tramas.

PROFINET IO

Este protocolo foi definido por vários fabricantes, sendo o mais importante a Siemens, e é mantido pela PROFIBUS Internacional.

Depois da definição PROFINET CBA, o passo seguinte foi a definição de um modelo de aplicação para o PROFINET IO baseado no PROFIBUS DP (tipo 3 do IEC 61158).

Num sistema deste tipo existem três tipos de dispositivos: os controladores IO, os dispositivos IO e o supervisor IO. Os controladores IO controlam os dispositivos IO com comunicação de dados cíclica através de um *buffer*. O supervisor IO gere o funcionamento dos componentes IO e dos controladores IO do sistema.

O ciclo de troca de dados entre os componentes de um sistema PROFINET IO é dividido nas seguintes fases de comunicação: IRT (Isochronous Real Time), RT (Real Time) e NRT (Non Real Time) (Figura 2.13) [18].

Na fase *Isochronous* a comunicação é escalonada no tempo: em cada tempo de offset a trama IRT é enviada de uma porta para outra sem interpretação do endereço por parte do switch. Nas fases seguintes os *switches* comportam-se como *switches standard* Ethernet, passando a comunicação a ser baseada no endereço. Primeiro são transmitidas as tramas RT durante a fase RT e quando esta termina é iniciada a fase NRT, durante a qual são transmitidas as tramas NRT.

Figura 2.13 - Ciclo de comunicação do PROFINET IO

2.7 Conclusão

Neste capítulo foram abordadas as redes de comunicação industriais, tendo sido feita uma análise aos principais protocolos actualmente utilizados.

Pode-se questionar sobre a necessidade do desenvolvimento de tantos protocolos. No entanto, tal facto é justificado, por um lado, pela pressão dos vários grupos económicos e, por outro, pela complexidade e variedade das possíveis áreas de aplicação.

Em relação a este segundo aspecto, é de facto difícil de conceber que uma única norma consiga abranger todas as áreas de aplicação e, nas várias tentativas feitas, provou-se que tal norma se tornava demasiado complexa, tendo um custo de implementação demasiado alto.

Quanto ao primeiro ponto, é evidente que as empresas fabricantes de sistemas e equipamento não tinham, e não têm, interesse em divulgar os protocolos de comunicação, para proteger os investimentos feitos em termos de I&D (Investigação e Desenvolvimento).

No entanto, depois de muitos anos de esforços foi adoptada uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 e o IEC 61784, que englobam as soluções comerciais mais importantes, incluindo soluções RTE.

Compete ao utilizador final e ao mercado decidir quais das soluções propostas preenchem os requisitos das aplicações em automação.

2 Redes de Comunicações Industriais

2.1 Introdução

A evolução da tecnologia nos últimos anos teve uma grande influência na sociedade, levando a caracterizá-la hoje como a sociedade do conhecimento. Com efeito, a globalização é hoje uma realidade, permitindo um rápido acesso à informação onde quer que ela se encontre, originando assim um esforço de actualização constante, já que a informação de que hoje dispomos ficará rapidamente ultrapassada.

O reflexo nas empresas fabris desta maneira de estar da sociedade actual traduz-se em novos desafios, no que respeita à produtividade: o nível de exigência do consumidor aumentou, os ciclos de vida dos produtos diminuíram, as linhas de produção tiveram de ser optimizadas em termos de níveis de *stocks* e flexibilidade, tudo a um baixo custo, para ser possível responder às necessidades do mercado de uma forma rentável. Este desafio nas áreas da inovação e da competitividade obrigou as empresas a concentrar esforços na modernização tecnológica dos seus processos de fabrico, nomeadamente na automatização dos mesmos. Deste esforço integrado resultaram, para além de produtos mais competitivos, o desenvolvimento de soluções tecnológicas avançadas que, à medida que se tornaram cada vez mais comuns e acessíveis, passaram também a ser incorporadas nos próprios processos de fabrico.

Durante as últimas três décadas assistiu-se a uma evolução sem paralelo na área dos sistemas de controlo, nomeadamente ao nível dos respectivos processos de concepção, implementação e operação. Isto deveu-se, em grande parte, aos novos desenvolvimentos, quer em áreas tecnológicas, tais como a microelectrónica e as telecomunicações, quer em áreas associadas à gestão e à integração de sistemas, bem como ao desejo de disponibilizar aos utilizadores finais equipamentos com maiores funcionalidades a custos mais reduzidos.

Este desenvolvimento reflectiu-se também ao nível das comunicações industriais, através da substituição progressiva das tradicionais comunicações ponto-a-ponto pelas

LANs (*Local Area Networks*). Embora inicialmente os motivos desta mudança estivessem relacionados com aspectos económicos, tais como a redução da cablagem e dos custos de manutenção, resultaram posteriormente em enormes vantagens ao nível da descentralização do controlo dos processos, na facilidade de instalação e configuração, na elevada flexibilidade de utilização e na melhoria do desempenho dos sistemas de controlo.

A crescente descentralização ao nível das funções de controlo e a crescente utilização de dispositivos inteligentes baseados em microprocessadores ou microcontroladores, criaram as condições necessárias para o desenvolvimento e proliferação das redes de campo. Estas são um tipo específico de rede local industrial, com o objectivo de interligar controladores, sensores e actuadores, que realizam a *interface* com o processo industrial.

Neste capítulo são analisadas as redes de comunicações industriais, com destaque para as redes de campo, os seus *standards* e as soluções comerciais ao nível das redes com fios. Neste contexto, na secção 1.2 é abordado o sistema de controlo do ambiente industrial, sendo ainda feito um resumo sobre a evolução das tecnologias de controlo. Na secção 1.3 é feita uma descrição do modelo OSI, uma vez que os *standards* de redes de campo são baseados nesse modelo. De seguida, na secção 1.4 é analisada a arquitectura das comunicações industriais, sendo ainda estabelecida uma relação entre esta e os níveis de controlo existentes num ambiente industrial. Na secção 1.5 são abordadas as redes de campo em particular, é feito um breve resumo sobre a história da standardização deste tipo de redes e são ainda apresentados os protocolos incluídos no conjunto de *standards* que especificam este tipo de redes. Por último, na secção 1.6 é abordada a *Ethernet* em tempo real e são apresentadas as soluções RTE (Real Time Ethernet) existentes.

2.2 O Sistema de controlo

O funcionamento de forma correcta e segura de um processo industrial de qualquer natureza é assegurado por intermédio de um sistema de controlo apropriado. Independentemente da dimensão ou da complexidade do processo em causa, o respectivo sistema de controlo pode ser decomposto em três subsistemas com funções bem definidas: o processo controlado, o controlador e o operador humano (Figura 2.1) [5].

Figura 2.1 - Sistema de controlo

O controlador é um equipamento que interage com o seu ambiente através de duas *interfaces* com características distintas:

- a *interface* com o processo controlado é definida como a *interface* de instrumentação;
- a *interface* com o operador humano é definida como a *interface* homem-máquina.
- A *interface* de instrumentação consiste num conjunto de sensores e actuadores que transformam os sinais físicos do processo controlado em sinais com características apropriadas para serem utilizados pelo controlador, e vice-versa. A *interface* homem-máquina consiste num conjunto de dispositivos de entrada e saída, que permitem a interacção com um operador humano. Tipicamente, esta interacção realiza-se ao nível da definição de parâmetros do processo e da supervisão da respectiva evolução.

A função do controlador é controlar a evolução do processo através da execução de um algoritmo de controlo adequado. A partir do processamento da informação obtida, quer directamente do estado do processo através da *interface* de instrumentação, quer fornecida pelo operador humano através da *interface* homem-máquina, o algoritmo de controlo produz um conjunto de comandos que são enviados para o processo através da *interface* de instrumentação. Para realizar estas funções o controlador dispõe de uma estrutura funcional, baseada na utilização de equipamentos adequados ao processo em causa, que suporta a execução do algoritmo de controlo.

Ao nível da estrutura funcional, estes sistemas de controlo podem ser classificados em três tipos de arquitecturas (Figura 2.2) [5].

- Centralizadas - o algoritmo de controlo é executado por um único equipamento;
- Descentralizadas - o algoritmo é executado num único equipamento, mas

algumas tarefas de processamento mais simples (ex. condicionamento e aquisição de sinais) são executadas por outros equipamentos de menor complexidade. Isto implica a existência de uma estrutura de comunicações que permita a interacção e a cooperação entre os vários equipamentos (ex. comunicações série ponto-a-ponto);

- Distribuídas - o algoritmo de controlo encontra-se distribuído por vários equipamentos de complexidade e natureza distintas. Tal como nas arquitecturas descentralizadas, é também necessário dispor de uma estrutura de comunicações adequada, sendo esta, contudo, comparativamente muito mais complexa (ex. rede de campo).

Figura 2.2 - Exemplos de arquitecturas de controlo

2.2.1 Evolução das Tecnologias de Controlo

O advento do computador no início dos anos 60 permitiu que estes passassem também a ser utilizados para implementar funções de controlo. O termo DCC (Direct Digital Control) foi utilizado na época para enfatizar o facto do controlo do processo ser realizado directamente pelo computador. O facto de serem programáveis proporcionou-lhes uma esmagadora vantagem em comparação com as tecnologias de lógica discreta utilizadas até ao momento. Um único equipamento (um computador) concentra em si, quer

as tarefas do controlador, quer as *interfaces* de instrumentação e de homem-máquina. No caso da *interface* de instrumentação, os sensores e actuadores são tipicamente ligados ao controlador através de ligações ponto-a-ponto analógicas (ex. anel de corrente). Em paralelo com este processo, tem também início nos finais do anos 60 o desenvolvimento de máquinas de controlo numérico e de *robots* industriais.

As arquitecturas de controlo desenvolvidas até esta época são essencialmente centralizadas. Contudo, as crescentes exigências da indústria, conjugadas com o desenvolvimento do microprocessador no início dos anos 70, permitiram uma evolução para as primeiras arquitecturas descentralizadas. Esta evolução efectuou-se segundo duas perspectivas [6]:

- uma ao nível das indústrias de processos, com o desenvolvimento dos DCS (Distributed Control Systems) com o objectivo de interligar hierarquicamente os equipamentos de controlo de menor complexidade (por exemplo controladores PID - Proportional Integral Derivative) aos equipamentos de maior complexidade (por exemplo mini-computadores);
- outra ao nível das indústrias de manufactura, onde o PLC, cujo desenvolvimento se deu no início dos anos 70, foi utilizado como elemento central das arquitecturas de controlo.

Em ambas as perspectivas, a interligação entre equipamentos era tipicamente realizada, quer através de ligações ponto-a-ponto analógicas, quer através de ligações digitais, utilizando neste último caso protocolos de comunicação proprietários. Embora esta evolução tenha permitido o desenvolvimento de sistemas de controlo cada vez mais complexos, durante a primeira década da sua utilização, as arquitecturas de controlo continuaram a ser caracterizadas por uma estrutura tipicamente centralizada e só mais tarde se registou uma evolução para soluções do tipo descentralizado.

Entre meados dos anos 80 e inícios dos 90, assistiu-se a uma alteração da estrutura das arquitecturas de controlo através da crescente utilização de redes de comunicação industriais para interligar os equipamentos de controlo. Esta evolução tecnológica foi o ponto de partida das primeiras arquitecturas de controlo descentralizadas baseadas numa estrutura de comunicações digital. Estas arquitecturas, embora mais complexas, permitiram obter um importante conjunto de vantagens, das quais se destacam: menores custos, melhores desempenhos, instalação e manutenção mais simples, modularidade, facilidade

na detecção de erros e avarias, etc. Na sequência desta evolução, surge também nesta época o conceito de CIM (Computer Integrated Manufacturing).

O CIM visa a cooperação entre os diferentes sistemas intervenientes no ambiente de fabrico e engloba todas as actividades com ele relacionadas, desde o projecto e desenvolvimento até ao *marketing* e vendas, passando pelo controlo do fabrico. Para que essa cooperação exista de facto é necessário que haja integração entre os sistemas. A integração significa a possibilidade de os subsistemas da empresa poderem interactuar entre si através de sistemas de comunicações de dados e bases de dados comuns.

Os sistemas de comunicações requerem infraestruturas técnicas (*software* e *hardware*). As comunicações requerem também regras (protocolos), regras essas condicionadas, não apenas por aspectos técnicos, mas também pela funcionalidade exigida.

Uma das representações da filosofia CIM consiste em decompor a empresa em cinco níveis, tal como a figura 2.3 indica.

Empresa	Decisões estratégicas Planeamento a longo prazo
Fábrica	Engenharia de concepção
Área	Controlo supervisor Planeamento de capacidades
Célula	Controladores de células SCADA
Posto de trabalho	Sistemas de controlo local sensores e actuadores

Figura 2.3 - Representação da filosofia CIM

A subdivisão em níveis é baseada, entre outros aspectos, nos tipos de actividades realizadas na empresa e leva, geralmente, ao uso de diferentes tipos de redes de comunicações nos vários níveis.

No interior de cada nível as comunicações horizontais são geralmente asseguradas por uma rede local. As comunicações verticais entre dois níveis adjacentes são resolvidas interligando as redes através de dispositivos de ligação.

A figura 2.4 representa um exemplo de uma arquitectura possível para a hierarquia de comunicações dentro de uma empresa.

Nos níveis superiores da hierarquia as comunicações podem ser caracterizadas como correspondendo à troca de grandes quantidades de informação, que tem de ser processada durante períodos relativamente longos mas com uma frequência relativamente baixa.

Ao contrário, nos níveis inferiores da hierarquia pequenas quantidades de informação precisam de ser processadas de uma forma rápida, com o objectivo de controlar processos industriais em tempo real. Este tipo de transacções tem normalmente uma periodicidade cíclica e uma frequência relativamente elevada.

Pode-se então concluir que não é possível satisfazer todos estes requisitos de transferência de dados com um só tipo de rede.

Figura 2.4 - Representação de uma arquitectura possível para a hierarquia das comunicações de uma empresa

Pode assim propor-se uma classificação hierárquica das comunicações industriais em três grandes grupos, que são: redes de fábrica, redes de célula e redes de campo.

As redes de fábrica abrangem os níveis superiores da hierarquia, enquanto as redes de campo correspondem ao nível mais baixo.

Embora esta evolução abrisse um conjunto enorme de perspectivas ao nível da integração de equipamentos situados em diferentes níveis de controlo, na prática isto acabou por não se verificar, devido ao desenvolvimento de muitas soluções proprietárias. Estas acabaram por limitar as potencialidades das arquitecturas de controlo, nomeadamente

ao nível da integração e da interoperabilidade entre equipamentos. Este problema colocou-se de forma especialmente grave ao nível das redes de campo, com os diferentes fabricantes a tentar impor as suas soluções como o *standard* a utilizar. São alguns exemplos o (PROcess FIeld BUS), o WorldFIP (Factory Instrumentation Protocol), o DeviceNet, o INTERBUS-S, e o AS-Interface (Application Server). Este processo terminou apenas recentemente através da adopção de uma solução de compromisso entre as várias propostas existentes [7]. Ao nível das arquitecturas de controlo registou-se uma tendência para adoptar soluções distribuídas, não só devido à possibilidade de dispor de equipamentos com maiores capacidades de processamento, mas também através do desenvolvimento de arquitecturas de comunicação que suportam elevados níveis de integração entre equipamentos.

Embora a introdução das redes industriais viesse resolver o problema da integração horizontal de equipamentos (situados no mesmo nível de controlo), a integração vertical (entre níveis de controlo) foi sempre um problema em aberto. As soluções apontadas inicialmente passavam pela utilização de equipamentos dedicados (*gateways*) ou pelo desenvolvimento de *software* específico que implementava as tarefas de mapear os serviços de comunicação das diferentes redes. Como estas soluções eram normalmente caras e complexas, surgiu no final dos anos 80 a ideia de desenvolver uma arquitectura de comunicações aberta baseada na estrutura do modelo OSI (*Open Systems Interconnection*). Exemplos destas soluções foram o MAP (Manufacturing Automation Protocol) e o MMS (Manufacturing Message Specification). No entanto, o seu sucesso acabou por ser limitado devido, quer à falta de suporte tecnológico adequado, quer à cumplicidade das soluções propostas.

Em paralelo, nas indústrias de processos a utilização de tecnologias SCADA (Supervisory Control and Data Aquisition) foi vista como uma alternativa mais simples e razoavelmente eficaz na integração vertical. Contudo, devido, quer à ausência de adequação destes sistemas para o problema em causa, quer à proliferação de equipamentos de controlo com características muito diversas, a utilização desta tecnologia acabou por resultar em soluções bastante limitadas.

Nos finais dos anos 90, devido às crescentes exigências de integração com aplicações de nível intermédio e superior, nomeadamente o ERP (Enterprise Resource Planning) e o MES (Manufacturing Execution System), foram desenvolvidas um conjunto de tecnologias de *software* baseadas em plataformas de objectos distribuídos, que disponibilizavam uma

infraestrutura ao nível dos serviços de comunicações, permitindo assim desenvolver de forma eficaz os conceitos de integração vertical e horizontal. São exemplos destas tecnologias o CORBA (Common Object Request Broker Architecture), com uma gama alargada de domínios de aplicação, e o OPC (Object linking and embedding for Process Control), que foi especialmente desenvolvido para satisfazer os requisitos no domínio das aplicações industriais. Este processo apresenta actualmente uma grande dinâmica, com destaque para o desenvolvimento de *standards* com base em arquitecturas de objectos distribuídos especialmente vocacionados para as necessidades dos ambientes industriais: IEC 61499 (Function Blocks for Industrial-Process Measurement and Control Systems) e o IEC 61804 (Function Blocks for Process Control). Como resultado deste trabalho, as arquitecturas de comunicação mais recentes já incorporam muitas destas funcionalidades, das quais se destacam: o CIP (Common Industrial Protocol), o IDA (Interface for Distributed Automation), o HSE *fieldbus* (High Speed Ethernet) e o PROFINET.

Entre os finais dos anos 90 e o início da corrente década verificou-se um fenómeno de migração de tecnologias de uso geral para a área das comunicações industriais. O caso mais paradigmático deu-se com a utilização da rede Ethernet em ambientes industriais (IE - Industrial Ethernet). Este processo teve um profundo impacto na estrutura das comunicações industriais, afectando todos os níveis de controlo. Esta migração deveu-se a vários factores, tais como: a existência de soluções de *hardware* de baixo custo e de elevado desempenho, bem como de protocolos de comunicação abertos e a disponibilização de plataformas de *software* para o desenvolvimento integrado de aplicações distribuídas.

A etapa mais recente desta evolução está centrada na utilização das tecnologias desenvolvidas para Web, tais como UDP/TCP/IP (User Datagram Protocol / Transmission Control Protocol / Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), XML (eXtensible Markup Language), Proxys, Java, ou Jini, para o desenvolvimento de aplicações industriais. A utilização destas tecnologias, para além de estarem largamente difundidas e do seu custo reduzido, vai permitir obter níveis de integração superiores nomeadamente ao nível dos domínios de aplicação externos ao ambiente industrial [11].

Associado ainda a este processo de migração de tecnologias emergentes para as redes industriais, é de salientar a crescente tendência para a utilização de redes de comunicações sem fios (como o IEEE 802.11 ou o IEEE 802.15) em ambientes industriais [9], [10].

2.3 O Modelo de Referência OSI

Convém agora, fazer uma descrição do modelo OSI, uma vez que os protocolos de comunicações industriais a seguir mencionados têm como referência esse modelo.

Num ambiente onde existem equipamentos provenientes de diferentes fabricantes a integração implica a definição de protocolos de comunicação normalizados. A ISO (International Organization for Standardization) definiu o modelo de referência OSI com o objectivo de promover o aparecimento de normas na área das comunicações entre computadores, equivalente ao que na altura se verificava já para as comunicações telefónicas, definidas no âmbito da CCITT (Commité Consultatif International de Telegraphique et Telephonique) [12]. O termo "sistema de arquitectura aberta" indica que se um sistema estiver conforme com o modelo OSI então está aberto a comunicar com qualquer outro que obedeça às mesmas normas. É de salientar que o modelo de referência OSI não especifica por si as normas de comunicação. O seu propósito é apenas fornecer uma arquitectura que sirva de base ao desenvolvimento de normas para sistemas de comunicação.

O modelo de referência OSI define 7 camadas, conforme se indica na figura 2.5.

Figura 2.5 - O modelo de referência OSI

A hierarquia dos níveis vai subindo, desde o nível de maior especificidade até ao mais alto, que é o nível mais genérico.

Os três primeiros níveis fornecem um serviço de rede, ou seja, tratam do transporte da informação. O nível físico trata do meio físico para a transmissão de *bits* de informação, o nível lógico organiza os *bits* de uma forma ordenada em blocos (tramas) e assegura que eles são transmitidos e recebidos de uma forma correcta, enquanto o nível de rede assegura que os pacotes chegam ao seu destino final.

Enquanto o serviço de rede fornecido pelos três níveis inferiores é adequado para transportar informação, algumas aplicações podem ter especificações que as redes não fornecem, como por exemplo uma taxa de erros baixa, um elevado nível de segurança, ou a necessidade de manter uma sequência de pacotes que façam uma mensagem completa. São estes os serviços que o nível de transporte fornece aos níveis superiores.

Os níveis acima do nível de transporte não tratam de mecanismos de transmissão de informação. Esse é o trabalho dos quatro níveis inferiores. No entanto, a informação necessita de ser sincronizada e tratada para que as aplicações entendam. O nível de sessão fornece o serviço de gestão da comunicação entre aplicações.

Outro ponto importante é o formato em que a informação é trocada. Os dois sistemas que estão a comunicar podem ter maneiras diferentes de representar os dados. O nível de apresentação preenche o requisito de identificar e estabelecer uma sintaxe comum, que será utilizada pelos dois sistemas.

O nível mais alto é o nível de aplicação, que constitui a *interface* entre as aplicações propriamente ditas e o sistema de comunicações.

Tendo sido feita uma introdução do modelo, a seguir é feita uma abordagem mais detalhada, especificando, em cada nível: os seus objectivos, os serviços oferecidos ao nível imediatamente superior e as suas funções.

2.3.1 O Nível Físico

O nível físico é responsável por uma transmissão transparente da informação através do meio físico. As funções do nível físico são inteiramente independentes do meio físico em uso, seja este constituído por fio de cobre, cabo coaxial ou fibra óptica. O tipo de meio físico utilizado é completamente escondido ao nível lógico pelo nível físico.

As definições do nível físico podem ser agrupadas da seguinte forma:

- Mecânicas: definem o tipo de conector, as dimensões físicas, as posições dos

pinos, etc;

- Eléctricas: definem as características eléctricas, como por exemplo: níveis eléctricos, impedância, etc;
- Funcionais: definem qual o significado dos níveis eléctricos em determinados pinos do conector;
- Procedimentais: definem as regras (procedimentos) a aplicar às várias funções e também qual a sequência em que determinados eventos podem ocorrer.

Serviços Fornecidos ao Nível Lógico

O nível físico fornece os seguintes serviços ao nível lógico:

- Ligações físicas: o fornecimento de uma transmissão de *bits* perfeitamente transparente entre entidades lógicas. A ligação física estabelece um “circuito de informação” entre dois pontos. A ligação física pode ser estabelecida entre dois pontos ou directamente, ou através de um sistema intermédio;
- Tratamento das unidades de informação: este serviço compreende a transmissão de um *bit* em transmissão série, ou de n *bits* em transmissão paralela. A ligação física pode ser *full-duplex* (a informação é feita nos dois sentidos simultaneamente), *half-duplex* (a informação é feita nos dois sentidos mas alternadamente), ou ainda *simplex* (a informação só é feita num sentido);
- Ligação entre pontos: a ligação entre pontos pode ser ponto-a-ponto ou multiponto;
- Sequenciamento: o nível físico coloca os *bits* no meio físico na mesma ordem que lhe foram fornecidos pelo nível lógico
- Identificação de circuito: o nível físico fornece identificadores que definem univocamente a ligação entre dois sistemas. O nível físico fornece identificadores da ligação entre pontos, que podem ser utilizados pelo nível lógico;
- Recuperação de falhas: o nível lógico é notificado de problemas detectados pelo nível físico;
- Parâmetros fornecidos ao nível lógico: são fornecidos parâmetros ao nível lógico, tais como: taxas de erro, taxas de transmissão, disponibilidade de serviço e atrasos.

Funções do Nível Físico

As seguintes funções são executadas pelo nível físico:

- Estabelecimento e libertação das ligações entre entidades do nível lógico;
- Transmissão de sequências de *bits*: estas podem ser síncronas ou assíncronas;
- Gestão: os protocolos do nível físico tratam de alguns aspectos relacionados com a gestão das actividades deste nível.

2.3.2 O Nível Lógico

O nível lógico isola os níveis superiores das características do meio de transmissão e fornece uma ligação sem erros e de confiança. O nível lógico é estabelecido sobre uma ou mais redes físicas e liga duas identidades em sistemas adjacentes. As ligações lógicas são ponto-a-ponto.

Dentro do nível lógico as sequências de *bits* do nível físico são organizadas em blocos de informação denominados tramas. São funções do nível lógico a sincronização dos *bits* dentro de uma trama, a detecção e correcção de erro (através da retransmissão de pacotes) e ainda o controlo de fluxo (dependendo do estado do sistema de recepção, liga ou desliga a transmissão de pacotes).

Serviços Fornecidos ao Nível de Rede

Os seguintes serviços são fornecidos pelo nível lógico:

- Ligação lógica: o estabelecimento de uma ou mais ligações entre duas entidades;
- Unidades de informação do nível lógico: estas entidades teóricas são mapeadas numa base de uma para uma em unidades do protocolo em uso. Na prática, estas são as tramas transmitidas numa ligação lógica;
- Identificadores lógicos: se requerido pelo nível físico, o nível lógico pode fornecer identificadores dos pontos da ligação lógica;
- Sequenciamento: manutenção da sequência correcta de pacotes;
- Detecção de erros: se for detectado um erro não recuperável pelo nível lógico, então o nível físico será notificado;
- Controlo de Fluxo: o nível de rede pode controlar dinamicamente a taxa a que pode receber os pacotes;
- Parâmetros da qualidade do serviço: estes parâmetros são opcionais e incluem

tempos médios entre erros detectados mas irrecuperáveis, taxa de erro residual, disponibilidade do serviço e débito.

Funções do Nível Lógico

As seguintes funções são efectuadas no nível lógico:

- Estabelecimento e libertação das ligações do nível lógico: como foi referido, esta função faz um mapeamento das unidades de informação em unidades do protocolo, em uso numa forma de uma para uma;
- Separação de ligações lógicas: esta função é feita dividindo uma ligação lógica em várias ligações físicas;
- Delimitação e sincronização: esta é essencialmente uma função de empacotamento, que organiza *bits* (unidades do nível físico) em tramas (unidades lógicas);
- Controlo de sequência: mantém a ordem sequencial dos pacotes transmitidos através da ligação lógica;
- Detecção de erros: esta função detecta erros de transmissão, de formato e de operação, que usualmente aparecem devido a deficiências no meio físico;
- Recuperação de erros: esta função tenta recuperar os erros, geralmente através da retransmissão de pacotes;
- Controlo de fluxo: fornece os serviços de controlo de fluxo já descritos;
- Identificação e troca de parâmetros: efectua a identificação de entidades lógicas e controla a troca de parâmetros;
- Controlo da ligação do circuito de dados: esta função fornece o nível de rede com a informação necessária para controlar e manter o circuito de dados ao nível de rede;
- Gestão: os protocolos do nível físico tratam de alguns aspectos da gestão das actividades deste nível.

2.3.3 O Nível de Rede

A função essencial do nível de rede é fornecer uma transmissão de dados perfeitamente transparente de um nível de transporte de um sistema (por exemplo uma aplicação num terminal) a um nível de transporte de outro sistema (por exemplo a aplicação servidora num computador central).

Em redes complexas, entidades comunicantes no nível de transporte não necessitam de estar próximas, mas ligadas através de um ou mais sistemas intermédios. Nestes casos, o nível de rede fornece funções de encaminhamento. Um exemplo pode ser a ligação de uma rede pública de dados com uma rede privada (por exemplo uma rede bancária) e uma rede local. Os endereços de rede são utilizados para identificar as várias entidades comunicantes no nível de transporte ao nível de rede.

Serviços Fornecidos ao Nível de Transporte

Os seguintes serviços são fornecidos pelo nível de rede:

- Endereços de rede: são fornecidos pelo nível de rede e são usados por entidades do nível de transporte, de forma a identificar univocamente outras entidades do nível de transporte;
- Ligações de rede: fornecem os meios de transferir dados entre entidades do nível de transporte;
- Identificadores de Ligações Rede entre sistemas: o nível de rede fornece às entidades do nível de transporte um identificador de ligação associado univocamente com o endereço de rede;
- Unidades de informação do nível de rede: numa ligação de rede o nível de rede fornece, para transmissão, unidades de informação (pacotes de dados). Estas unidades têm um cabeçalho e um final perfeitamente definidos. A integridade da unidade é verificada no nível de rede;
- Parâmetros de qualidade do serviço: estes parâmetros incluem taxa residual de erros, disponibilidade do serviço, habilidade, débito, atraso no tráfego e atraso no estabelecimento de ligações na rede;
- Notificação de erros: erros irrecuperáveis para o nível de rede são participados ao nível de transporte;
- Sequenciamento: o nível de rede pode fazer a entrega de unidades de informação do nível de rede sequencialmente para uma determinada ligação de rede;
- Controlo de fluxo: a entidade de transporte que está a receber pode fazer com que o Serviço de Rede pare de enviar mais unidades de informação. Este controlo de fluxo pode ou não ser enviado ao outro extremo da ligação;
- Libertação: a entidade de transporte pode pedir a libertação da ligação.

Funções do Nível de Rede

As funções de nível de rede fornecem uma grande variedade de configurações, desde ligações ponto-a-ponto a ligações mais complexas, com uma combinação de várias sub-redes. As seguintes funções são efectuadas:

- Encaminhamento e repetição: as ligações da rede são fornecidas por entidades nos sistemas finais, mas podem ser envolvidas entidades em sistemas intermédios que façam repetição. As funções de encaminhamento determinam um caminho definido entre dois endereços;
- Ligações de rede: esta função fornece ligações entre entidades do nível de transporte, fazendo uso de ligações fornecidas pelo nível lógico;
- Multiplexação de ligações de rede: esta função é usada para multiplexar ligações de rede em ligações lógicas;
- Segmentação e empacotamento: o nível de rede pode segmentar e/ou formar blocos que constituem unidades de informação do nível de rede, para facilitar o transporte;
- Funções de detecção de erros: são utilizadas para verificar se a qualidade dos serviços fornecidos numa rede é mantida. Quando há detecção de erros no nível de rede o nível lógico é notificado. As funções de recuperação de erros dependem da qualidade do Serviço de Rede fornecido;
- Sequenciamento: prevê a entrega sequencial de unidades de informação do Serviço de Rede numa determinada ligação;
- Controlo de fluxo;
- Selecção de serviços: esta função permite que sejam seleccionadas as mesmas funções nos dois sistemas, mesmo quando a ligação se faz entre vários subsistemas.

2.3.4 O Nível de Transporte

O papel do nível de transporte é complementar a rede que está por baixo, de forma a assegurar a qualidade dos serviços requeridos que estão acessíveis ao utilizador.

As funções do nível de transporte estão focalizadas em optimização de custos, controlo de erros, controlo de fluxos, sequenciamento e multiplexagem. O nível de transporte também verifica a existência de duplicados e perdas de informação. Se a ligação de rede for quebrada temporariamente, a ligação de transporte pode ser mantida até que a ligação seja restaurada.

Os protocolos do nível de Transporte são definidos para aceitar uma grande variedade de redes, com várias qualidades de serviços. São cinco as classes de Serviços de Transporte disponíveis:

- A classe 0 é a classe mais simples, sem melhoramentos nos Serviços de Rede;
- A classe 1 adiciona recuperação de erros para redes sujeitas a uma grande frequência de interrupções;
- A classe 2 tem as funções da classe 0 mais multiplexagem;
- A classe 3 tem as funções da classe 1 mais multiplexagem;
- A classe 4 adiciona funções de detecção de erros e de dados fora de sequência.

Serviços Fornecidos ao Nível de Sessão

Os seguintes serviços são fornecidos pelo nível de transporte:

- Estabelecimento de ligações de transporte: as ligações de transporte são estabelecidas entre identidades do nível de sessão e são identificadas pelo endereço de transporte. A qualidade do serviço é negociada entre as entidades do nível de sessão e o serviço de transporte;
- Transferência de dados: fornece a transferência de dados, de acordo com a qualidade de serviço que foi negociada;
- Libertação da ligação de transporte: fornece meios para que qualquer entidade da camada de sessão dos sistemas possa libertar a ligação de transporte.

Funções do Nível de Transporte

As operações no nível de transporte são:

1 Fase de Iniciação

Durante esta fase são efectuadas as seguintes funções:

- Obtenção de uma ligação à rede que corresponda aos requisitos em termos de custos e qualidade de serviço.
- Decisão de multiplexagem ou divisão.
- Estabelecer as unidades de informação do protocolo de transporte óptimas.
- Selecção das funções que devem estar operacionais durante a transferência de dados.
- Mapeamento dos endereços de transporte em endereços de rede.

- Fornecimento de identidade aos endereços de transporte.
- Transferência dos dados.

2 Fase de Transferência

Durante esta fase é executada a transmissão de unidades de informação do protocolo de transporte. Os seguintes serviços podem ser usados ou não, dependendo da classe de serviço seleccionada:

- Sequenciamento;
- Empacotamento;
- Segmentação;
- Multiplexagem ou divisão;
- Controlo de fluxo;
- Detecção e recuperação de erros;
- Transferência dos dados enviados;
- Delimitação das unidades de informação do serviço de transporte;
- Identificação das ligações de transporte.

3 Fase de Libertação

Esta fase inclui as seguintes funções:

- Notificação das razões da libertação.
- Identificação da ligação de transporte libertada.
- Transferência de dados.

2.3.5 O Nível de Sessão

Os requisitos para o nível de sessão reflectem a observação da utilização dos sistemas, pela maior parte dos utilizadores, em picos de actividade que podem ser chamados de sessões. Durante a sessão, o utilizador e o sistema iniciam um diálogo. A primeira função do nível de sessão é estabelecer, manter e gerir este diálogo.

As ligações da camada de Sessão são mapeadas em ligações da camada de transporte numa razão de um para um. Não existe multiplexagem neste nível, mas é possível que várias ligações de sessão usem a mesma ligação de transporte sequencialmente. Simultaneamente, uma ligação de sessão pode usar mais que uma ligação de transporte. Se a ligação de transporte se quebrar, devido a problemas nas camadas inferiores da rede, é possível estabelecer uma nova ligação de transporte sem a intervenção do utilizador ou

mesmo chegar ao seu conhecimento a quebra. Neste caso é o nível de sessão que é o responsável pela ressincronização do diálogo entre os dois sistemas.

Serviços Fornecidos ao Nível de Apresentação

Os seguintes serviços são fornecidos pelo nível de sessão:

- Estabelecimento da ligação entre níveis de sessão: permite que duas entidades do nível de apresentação possam estabelecer uma ligação de sessão entre elas;
- Libertação de ligação: permite que entidades do nível de apresentação possam libertar uma ligação do nível de sessão de uma forma ordeira e sem perda de informação;
- Transferência de dados: permite que uma entidade emissora do nível de apresentação possa transferir uma unidade de informação do nível de sessão a uma entidade receptora do nível de apresentação;
- Serviço de Quarentena: permite à entidade emissora solicitar que algumas unidades de informação, enviadas por uma conexão do nível de sessão, não devam ser enviadas à entidade receptora do nível de apresentação, até ordem contrária enviada pelo emissor;
- Gestão de Interacção: permite que entidades do nível de apresentação comandem explicitamente quem vai controlar certas funções de controlo. São possíveis os seguintes tipos de interacção: dois sentidos simultaneamente, dois sentidos alternadamente, um sentido;
- Sincronização de ligação: este serviço permite que entidades do nível de apresentação definam e identifiquem pontos de sincronização que obriguem uma ligação do nível de sessão a permanecer num determinado estado (*reset*) e que definam qual o ponto de ressincronização;
- Situações excepcionais: faz a notificação ao nível superior de quaisquer situações não englobadas pelos serviços deste nível.

Funções do Nível de Sessão

A maior parte das funções necessárias neste nível estão implícitas aos serviços deste nível:

- Mapeamento das ligações de sessão às ligações de transporte;
- Controlo do fluxo do nível de sessão: o nível de sessão não possui controlo de fluxo. Para evitar aumentar as funções do nível de sessão este controlo é feito no nível de

transporte;

- Recuperação de ligações quebradas: no caso de quebra de ligação do nível de transporte o nível de sessão pode ter as funções necessárias para restabelecer uma nova ligação, de forma a continuar a sessão;
- Libertação da ligação de Sessão: permite que se acabe e liberte a ligação sem perda de informação.

2.3.6 O Nível de Apresentação

Este nível é responsável por assegurar que a informação é apresentada ao utilizador de uma forma útil (através do nível de aplicação). O nível de apresentação só trata da sintaxe da informação (a forma como é representada a informação) e não com a sua semântica (significado da informação).

Serviços Fornecidos ao Nível de Aplicação

Os seguintes serviços são fornecidos pelo nível de apresentação:

- Transformação da Sintaxe: trata dos códigos e do conjunto de caracteres a usar (por exemplo o código ASCII), bem como da apresentação da informação (por exemplo a visualização da informação num monitor);
- Selecção da Sintaxe.

Funções do Nível de Apresentação

As funções do nível de apresentação são:

- Negociação e Renegociação da Sintaxe;
- Transformação da Sintaxe;
- Gestão da passagem de serviços dos Níveis Sessão e Aplicação.

2.3.7 O Nível de Aplicação

O nível de apresentação constitui o *interface* entre as aplicações propriamente ditas e o sistema de comunicação. As aplicações trocam informação entre si, utilizando entidades e protocolos do nível de aplicação e serviços do nível de apresentação.

Serviços Fornecidos às Aplicações

Além da transferência da informação, estes serviços podem incluir:

- Identificação dos vários intervenientes da comunicação através do nome, endereço e descrição;
- Determinação da disponibilidade dos intervenientes;
- Verificação e validação dos intervenientes;
- Determinação dos recursos necessários;
- Determinação da qualidade de serviço mínima;
- Sincronização de aplicações;
- Selecção da forma de diálogo;
- Entendimento na responsabilidade na recuperação de erros;
- Acordo na forma de controlo da integridade da informação;
- Identificação de limitações na sintaxe da informação.

Funções do Nível de Aplicação

O nível de aplicação contém todas as funções exigidas pela comunicação entre sistemas abertos, mas que não são fornecidas pelos níveis inferiores. As comunicações entre aplicações são efectuadas através de entidades do nível de aplicação. Estas entidades representam conjuntos de capacidades de comunicação OSI e estão divididas em elementos específicos implementados pelo utilizador e elementos pertencentes aos serviços do nível de aplicação, sendo estes últimos denominados por ASE (Application Service Element).

Um exemplo de um serviço do tipo ASE é o MMS (Manufacturing Message Specification), que é uma norma internacional do nível de aplicação vocacionada para o ambiente industrial.

2.4 A Arquitectura das Comunicações Industriais

Ao nível dos sistemas de controlo a integração implica a necessidade de cooperação e interacção entre os vários subsistemas incluídos no mesmo sistema. Isto significa transferência, armazenamento e processamento de informação em ambientes com características heterogéneas, o que por sua vez obriga à necessidade de dispor de uma infra-estrutura de comunicações adequada. As redes locais industriais, não sendo a solução para este problema, são contudo uma parte integrante e essencial dessa solução.

Os fluxos de informação existentes num ambiente industrial possuem características de tal forma distintas que não é possível dispor de uma única rede capaz de satisfazer todas

as necessidades de comunicação. Desta forma, a alternativa é dispor de um conjunto de redes que no seu conjunto sejam capazes de satisfazer a totalidade dessas necessidades. Num sistema automatizado as actividades relacionadas com o controlo do processo industrial podem ser estruturadas num modelo hierárquico caracterizado por fluxos de informação verticais entre entidades de níveis hierárquicos adjacentes e por fluxos de informação horizontais entre entidades do mesmo nível hierárquico. Como estas actividades estão intimamente associadas à estrutura de comunicações que lhes serve de suporte, surge de forma natural a adopção de um modelo hierárquico para a arquitectura de comunicações (Figura 2.6) [5].

Figura 2.6 - Relação entre os níveis de controlo e a arquitectura de comunicações

Embora os modelos hierárquicos para a estrutura de controlo possam variar em número de níveis, tipicamente entre o 4 e o 6, ao nível da arquitectura de comunicações é usual identificar três níveis distintos: fábrica, célula e campo. Para cada um destes níveis foram desenvolvidas várias soluções, cada uma possuindo diferentes objectivos, protocolos, capacidades e complexidade:

- Fábrica - Cobrem as necessidades dos níveis superiores. As principais actividades encontradas a este nível são o planeamento da produção, de processos e de materiais e as áreas de engenharia financeira e comercial. O fluxo de informações descendente centra-se essencialmente nas ordens de fabrico e nas informações associadas ao seu escalonamento. No sentido ascendente circulam informações relativas ao estado das ordens de fabrico, à qualidade do processo produtivo e a pedidos de aquisição de materiais e/ou recursos. Este nível é caracterizado por um elevado fluxo de informação horizontal entre e dentro dos vários subsistemas existentes sem requisitos temporais críticos.

- Célula - Cobrem as necessidades dos níveis intermédios. Uma célula agrupa um conjunto de equipamentos que cooperam para a execução de uma determinada tarefa. As principais actividades encontradas a este nível são o escalonamento, o sequenciamento e a execução de tarefas. Outras actividades também executadas têm a ver com a compilação da informação relativa à qualidade da produção e ao desempenho dos equipamentos que constituem a célula. A informação que circula do nível célula para os níveis descendentes inclui ordens de execução de operações ou programas de controlo, no caso de equipamentos programáveis. Em sentido ascendente a informação disponibilizada diz respeito à evolução das operações executadas e aos resultados dessas mesmas operações. Este nível é caracterizado por fluxos de informação de volume intermédio e com requisitos temporais exigentes, que em muitos casos podem ser críticos.
- Campo - Cobrem as necessidades dos níveis mais baixos. As principais actividades encontradas a este nível estão relacionadas com o controlo directo do processo industrial, nomeadamente a execução de algoritmos de controlo, por equipamentos que actuam fisicamente sobre os materiais ou produtos a operar. A *interface* com o processo é realizada por intermédio de sensores e actuadores, muitos deles dotados de capacidades de processamento complexas (*smart sensors*). Este nível é caracterizado por fluxos de informação de pequeno volume e com requisitos temporais críticos.

2.5 Redes de Campo

As redes de campo foram inicialmente desenvolvidas com o objectivo de satisfazer os requisitos de comunicação dos níveis mais baixos das arquitecturas de controlo industriais. Entre estes destacam-se, pela sua importância, os seguintes [14], [15]:

- Capacidade de transferir pequenos volumes de informação de forma eficiente;
- suportar tráfego periódico (por exemplo amostragem de dados) e aperiódico (por exemplo eventos) com tempos de resposta majorados. Existem assim requisitos de tempo real associados às comunicações;
- capacidade de operar em ambientes industriais típicos, sujeitos a interferências electromagnéticas, vibrações, corrosão, poeiras, humidade, etc;
- garantir um nível adequado de confiança no funcionamento, nomeadamente no que diz respeito à fiabilidade, disponibilidade e segurança e
- baixo custo de aquisição, instalação, operação e manutenção.

De forma a satisfazer estes requisitos foi adoptada uma *stack* de comunicação organizada de acordo com o modelo OSI, mas compactada em 3 níveis: físico, ligação de dados e aplicação. O nível de aplicação incorpora algumas funcionalidades definidas nos restantes níveis não utilizados neste modelo.

Para cada um dos níveis podem ser definidos múltiplos serviços e protocolos de comunicação com características muito diversas. A escolha destes elementos resulta essencialmente dos objectivos originais definidos pelos fabricantes das redes de campo, que de uma forma sucinta podem ser expressos segundo duas perspectivas [15]:

- A rede de campo é considerada apenas como uma forma de simplificar as ligações físicas entre os vários dispositivos ou
- a rede de campo é considerada a coluna vertebral (*backbone*) de um sistema distribuído e de tempo-real.

A diferença entre estas duas perspectivas foi uma das razões que levaram à proliferação de soluções para as redes de campo. Outras razões estão relacionadas com a ausência de um *standard* internacional único e genérico.

2.5.1 Standardização das Redes de Campo

Já no início dos anos 70 foram instaladas e utilizadas as primeiras redes de campo. No entanto, o trabalho de standardização só teve início em meados dos anos 80. A ideia básica de um *standard* é estabelecer uma especificação de uma forma muito rígida e formal, excluindo a possibilidade de pequenas alterações. Isto dá uma certa noção de confiabilidade e estabilidade da especificação, que por sua vez assegura a confiança dos utilizadores e consequentemente uma boa posição no mercado. Além disso, em muitos países os *standard*s têm uma posição *legally binding*, o que significa que quando um *standard* pode ser aplicado é obrigatório aplicá-lo. Isto implica que um sistema standardizado ganha uma posição competitiva em relação aos rivais não standardizados. Não é então de admirar que fosse iniciada uma corrida para a standardização.

A standardização internacional das redes de campo foi sempre difícil. Teve o seu início em 1985 e, depois de uns anos entusiásticos de desenvolvimento, a procura de um único *standard* foi ficando enredada numa rede de políticas de companhias e de interesses de *marketing* [7].

Na segunda parte dos anos 80, no início dos trabalhos da comissão técnica TC 65C do IEC (International Electrotechnical Commission) o desenvolvimento dos sistemas

fieldbus foi basicamente um projecto europeu, levado a cabo, não só por investigadores com um *background* académico, mas também por muitos proprietários. Os resultados mais promissores foram o francês FIP e o alemão PROFIBUS. Ambos foram standardizados a nível nacional e posteriormente propostos ao IEC para standardização internacional. No entanto, as abordagens dos dois sistemas eram completamente diferentes. O PROFIBUS baseava-se no controlo distribuído e a sua forma original suportava uma comunicação vertical orientada ao objecto, de acordo com o modelo cliente-servidor, no espírito da especificação MAP/MMS. Por outro lado, o FIP foi desenvolvido segundo um esquema de controlo centralizado mas capaz de suportar comunicação em tempo real, de acordo com o novo modelo para comunicação horizontal produtor-consumidor ou *publisher-subscriver*.

Como eram muito diferentes, os dois sistemas satisfaziam os requisitos de áreas de aplicação diferentes. Evidentemente, um *fieldbus* universal tinha de combinar os benefícios dos dois, pelo que um grupo de peritos apresentou uma nova proposta, o WorldFIP, que é uma extensão do FIP ao qual foi acrescentada a funcionalidade do modelo cliente-servidor. Por outro lado, o ISP (Interoperable System Project) tentou demonstrar que o PROFIBUS poderia ser melhorado com a introdução do modelo de comunicação *publisher-subscriber*. No entanto o ISP foi abandonado em 1994 por razões estratégicas [7].

Ao mesmo tempo, o papel de líder nos trabalhos de standardização ao nível do IEC foi sendo tomado, não pelos europeus, mas pelo comité SP50 do ISA (International Society of Automation), que foi muito mais eficiente no fim dos anos 80 e teve uma influência importante na estrutura de camadas do *standard* actual. No entanto, até meados dos anos 90 o comité do IEC não tinha produzido nenhum resultado substancial durante mais de 8 anos. A única excepção foi a definição da camada física, que foi adoptada como um *standard* IEC 61158-2 em 1993.

Em 1995, depois de longos anos de disputas entre investigadores alemães e franceses, com vista a combinar as abordagens FIP e PROFIBUS, várias companhias, basicamente americanas, decidiram não continuar a testemunhar as infindáveis discussões. Com o fim do projecto ISP, iniciaram a definição de uma nova rede de campo optimizada para a indústria de processos: o FF (Fieldbus Foundation). Este trabalho foi feito à parte dos comités IEC, dentro do ISA, e por algum tempo o trabalho no IEC pareceu posto de parte.

A 15 de junho de 1999 o comité de acção do IEC decidiu tomar um novo rumo e um mês depois, a 16 de Junho, os representantes das principais partes interessadas na

standardização *fieldbus* (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, PROFIBUS User Organization e Siemens) assinaram um "Memorando de Entendimento", com o objectivo de pôr um ponto final na disputa dos *standards fieldbus*.

Este processo culminou em 2003 com a adopção de uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 (Digital Data Communications for Measurement and Control - Fieldbus for use in Industrial Control Systems) e o IEC 61784 (Digital Data Communications for Measurement and Control - Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems), sendo ambos constituídos por um conjunto de perfis de comunicação, aos quais acabaram por corresponder as soluções comerciais mais importantes existentes à data da sua publicação (Tabela 2.1) [7].

Tabela 2.1 - Perfis e protocolos de acordo com o IEC 61784 e o IEC 61158

IEC 61784 Perfil	IEC 61158 Protocolos-camadas			Standard CENELEC	Nome comercial
	Física	Ligação de dados	Aplicação		
CPF-1/1	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H1)
CPF-1/2	Ethernet	TCP/UDP/IP	Tipo 5	-	Foundation Fieldbus (HSE)
CPF-1/3	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H2)
CPF-2/1	Tipo 2	Tipo 2	Tipo 2	EN-50170-A3	ControlNet
CPF-2/2	Ethernet	TCP/UDP/IP	Tipo 2	-	Ethernet/IP
CPF-3/1	Tipo 3	Tipo 3	Tipo 3	EN-50254-3	PROFIBUS-DP
CPF-3/2	Tipo 1	Tipo 3	Tipo 3	EN-50170-A2	PROFIBUS-PA
CPF-3/3	Ethernet	TCP/UDP/IP	Tipo 10	-	PROFINET
CPF-4/1	Tipo 3	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-485
CPF-4/1	Tipo 1	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-232
CPF-5/1	Ethernet	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS)
CPF-5/2	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS, subMMS)
CPF-5/3	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS)
CPF-6/1	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS
CPF-6/2	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS TCP/IP
CPF-6/3	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS Subset
CPF-7/1	Tipo 1	Tipo 6	-	-	Swiftnet transport
CPF-7/2	Tipo 1	Tipo 6	Tipo 6	-	Swiftnet full stack

Como se pode verificar pela tabela, sistemas *fieldbus* simples, como o CAN e o AS-*Interface*, não foram incluídos nesta norma. Estes estão incluídos num *standard* específico para este tipo de sistemas, o IEC 62026 (Low-voltage switchgear and controlgear - Controller-Device Interfaces), publicado em Junho de 2007.

À medida que o processo de standardização foi estabilizando, o desenvolvimento focou-se na definição de uma quarta camada, denominada camada de utilizador. O seu objectivo é disponibilizar ao utilizador uma abordagem integrada no desenvolvimento das aplicações, nomeadamente através da definição de blocos funcionais, linguagens de descrição dos dispositivos, interoperabilidade e métricas da qualidade de serviço.

Quanto ao seu posicionamento em relação aos níveis de controlo das aplicações industriais, as redes de campo sofreram uma evolução, passando também a ser utilizadas presentemente como redes de célula. A própria terminologia tem evoluído, através da definição de um conjunto de subcategorias para as redes de campo (Figura 2.7) [5]. Neste sentido, o termo original *fieldbus* tem sido utilizado para designar as redes de campo que estão mais próximas do conceito de rede de célula (ex. PROFIBUS-DP, WorldFIP) e o termo *sensorbus* para designar as redes mais básicas e mais próximas do conceito original de rede de campo (ex. AS-Interface, INTERBUS-S), enquanto o termo *devicebus* é utilizado para designar as que estão num plano de actuação intermédio (ex. DeviceNet, FF-H1). Contudo, e por uma questão de simplificação de linguagem, utiliza-se nesta dissertação apenas os termos rede de campo ou *fieldbus* para representar todas as subcategorias acima definidas.

Figura 2.7 - Categorias das redes de campo

2.6 Ethernet em Tempo Real

Ao mesmo tempo que decorria a standardização *fieldbus*, no mundo administrativo eram implementadas redes baseadas na Ethernet e no TCP/IP. Os custos associados a estas

infra-estruturas têm vindo continuamente a baixar e tornou-se possível ligar quase tudo, em qualquer lado do mundo, com a ajuda da tecnologia da Internet. No entanto, no campo da automação, ainda eram utilizados *fieldbuses* dedicados, a única barreira para aceder a componentes no chão de fábrica via Internet.

Depois de mais de 1 década de experiência com aplicações de *fieldbuses* a indústria começou a desenvolver e a adoptar soluções RTE. Os *standard*s propostos pelo IEC tentam traçar uma linha de orientação e critérios de selecção baseados em indicadores reconhecidos.

A adopção da tecnologia Ethernet na comunicação industrial pressupõe capacidades Internet, como por exemplo *interfaces* com o utilizador remotos, via Web. No entanto, é uma solução inaceitável se a adopção da tecnologia Ethernet causa perda de características necessárias no chão de fábrica, tais como [18]:

- Comunicação determinística;
- acções sincronizadas entre componentes e
- troca de pequenos pacotes de dados eficiente e frequente.

Um requisito implícito e essencial é a capacidade de comunicação Ethernet no nível de escritório ser totalmente absorvida, de modo que o *software* de comunicação envolvido possa ser utilizado. Isto resulta nos seguintes requisitos:

- Suporte de migração da Ethernet do nível do escritório para RTE e
- uso de componentes *standard* (*bridges*, controladores Ethernet e *stack*s de protocolo).

Para se obter a necessária alta qualidade de transmissão de dados, com *jitter* limitado e com perturbações devidas ao tráfego de dados TCP/IP limitadas é necessário desenvolver novos componentes de rede.

Resumindo, a RTE é uma especificação *fieldbus* que utiliza a Ethernet nos dois níveis mais baixos.

2.6.1 Standardização RTE

O *standard* Ethernet não atinge os requisitos do RTE. Existem diferentes propostas na comunidade de investigação para a modificação da tecnologia Ethernet. O mercado também adoptou soluções técnicas adicionais. A seguir são apresentadas as soluções RTE propostas para standardização.

As *interfaces* de comunicação estão estruturadas em diferentes níveis. Na figura 2.8 estão representadas as estruturas possíveis de um protocolo de comunicação RTE [18]. Comum a todas as redes Ethernet é a infraestrutura de cablagem universal.

As aplicações *non real time* utilizam os protocolos Ethernet, tal como definido no ISO 8802-3, e o protocolo TCP/UDP/IP. Utilizam ainda protocolos típicos da Internet, tal como o HTTP ou o FTP.

Figura 2.8 - Estruturas possíveis de uma RTE

Para uma solução RTE existem três diferentes abordagens:

- Na primeira mantêm-se os protocolos TCP/UDP/IP e a modificação que garante o tempo real é feita no nível mais alto. É a solução *on top of* TCP/IP.
- Na segunda não são utilizados os protocolos TCP/UDP/IP e a funcionalidade Ethernet é acedida directamente. É a solução *on top of Ethernet*.
- Na terceira abordagem o mecanismo Ethernet e a própria infraestrutura são modificados de forma a obter uma *performance* em tempo real. É a *Modified Ethernet*.

Na secção seguinte são apresentados os protocolos RTE que existem no mercado.

2.6.2 Protocolos RTE

O IEC 61784-2 (Industrial Communication Networks - Profiles – Part 2: Additional Fieldbus Profiles for Real time Networks based on ISO/IEC 8802-3) é o documento *standard* que especifica pelo menos dez diferentes soluções técnicas para RTE, sendo muitas delas incompatíveis [18] (Tabela 2.2). Alguns dos protocolos propostos apenas

estão definidos, não existindo ainda produtos no mercado. No caso de outros protocolos já existem produtos e aplicações.

Tabela 2.2 - Perfis RTE definidos no IEC 61784

Perfil IEC 61784	**Nomes comerciais**	***Ethertypes***
CPF-2	ControlNet (Ethernet/IP)	(0x0800 IP)
CPF-3	PROFIBUS/PROFINET	0x8892
CPF-4	P-NET	(0x0800 IP)
CPF-10	Vnet/IP	(0x0800 IP)
CPF-11	*TCnet* (Time Critical control network)	0x888B
CPF-12	EtherCAT	0x88A4
CPF-13	EPL (Ethernet PowerLink)	0x88AB
CPF-14	EPA (Ethernet for Plant Automation)	0x88BC
CPF-15	MODBUS – RTPS (Real Time Publisher Subscriber).	(0x0800 IP)
CPF-16	SERCOS (SErial Real time COmmunication System Interface)	0x88CD

Protocolos *on top of* TCP/IP

Algumas soluções RTE utilizam a *stack* do protocolo TCP/UDP/IP sem modificações. Com esta *stack* é possível comunicar de uma forma transparente para além dos limites da rede de campo.

É então possível implementar redes de campo que comuniquem com todos os pontos do mundo, da mesma forma que a tecnologia Internet. No entanto, o manuseamento desta *stack* de protocolo de comunicação requer recursos razoáveis, quer ao nível do processamento, quer ao nível da memória e introduz atrasos não determinísticos na comunicação.

A seguir são apresentadas algumas soluções disponíveis no mercado.

Modbus/TCP

Foi definido pela Schneider Electric e é mantido pela Modbus-IDA. Utiliza o já conhecido Modbus (o *standard* industrial “de facto” desde 1979) sobre uma rede TCP/IP, através da porta 502.

Esta é provavelmente uma das soluções Ethernet mais utilizadas em aplicações industriais e satisfaz os requisitos da classe mais baixa de aplicações, o controlo humano.

É um protocolo muito simples, do tipo *request/reply* (envia uma trama de *request* e recebe uma trama de *reply*). Em adição ao histórico Modbus, este protocolo tem definidas extensões *real time* que utilizam o RTPS. O RTPS prevê dois modelos de comunicação: o

publisher-subscriber, que transfere dados do *publisher* para o *subscriber*, e o CST (Composite State Protocol), que transfere informação de estado de um escritor para um leitor.

Ethernet/IP

Este protocolo foi definido pela Rockwell e é mantido pela ODVA (Open DeviceNet Vendor Association) e pela ControlNet International. Utiliza o CIP, que é comum nas redes Ethernet/IP, ControlNet e DeviceNet.

Este protocolo está incluído no *standard* IEC 61784-1 como CP 2/2 (tipo 2 no IEC 61158) e fornece comunicação *real time* baseada no ISO/IEC 8802-3.

Na Ethernet *full-duplex* não existe a possibilidade de atrasos devidos a colisões. No entanto, as tramas Ethernet podem sofrer atrasos no próprio dispositivo de *switch*, caso a porta de saída esteja ocupada na transmissão de outra trama. Isto pode levar a atrasos não determinísticos, que não são aconselháveis em aplicações em tempo real. Para evitar estes atrasos está definido um mecanismo de prioridades no IEEE 802.3, que permite a atribuição de níveis de prioridade (0 a 7) a tramas Ethernet.

P-NET

O P-NET sobre a especificação IP foi proposto pelo comité nacional dinamarquês e o seu uso destina-se ao ambiente IP. Neste protocolo a comunicação em tempo real P-NET é embebida em pacotes UDP/IP, que tanto podem circular em redes IP como em redes *non* IP.

Uma trama P-NET inclui uma tabela P-Net *route*, que por sua vez é constituída por dois elementos: os endereços da fonte e do destino da própria trama. No caso mais simples de uma rede de campo, estes são os endereços de dois nós da própria rede. Para permitir a comunicação entre dispositivos da rede de campo e dispositivos de uma rede IP os endereços da tabela P-Net *route* terão de ser endereços IP.

De facto, este protocolo apenas especifica a forma como são integradas redes P-NET e redes UDP/IP e não prevê nenhuma medida que assegure um comportamento em tempo real na rede Ethernet.

Vnet/IP

Este protocolo foi desenvolvido pela Yokogama.

Utiliza o TCP/IP para a integração de protocolos Internet, como o HTTP, e de extensões de protocolos *real time*, o RTP (Real Time and reliable datagram Protocol).

Este não é de facto um protocolo RTE, apenas utiliza o protocolo UDP/IP para o transporte do protocolo RTP. Não são tomadas nenhumas medidas especiais que garantam o comportamento determinístico de um protocolo *real time*.

Protocolos *on top of* Ethernet

Estes protocolos RTE não alteram o *hardware* de comunicação Ethernet, mas especificam um tipo de protocolo especial na trama Ethernet, o *Ethertype* (tabela 2.2). Por exemplo, o tipo *standard* para o protocolo IP é *Ethertype*=0X0800. Estes protocolos RTE utilizam, além da *stack* de protocolo IP *standard*, a sua própria *stack* de protocolo identificada com o seu próprio tipo. A tabela 2.2 lista os diferentes valores assignados para as várias soluções.

EPL

Foi definido por Bernecker & Rainer e é mantido pelo grupo de standardização EPL.

Baseia-se num sistema de escalonamento *master-slave* num segmento Ethernet partilhado, o SCNM (Slot Communication Network Management). O *master* é o MN (Managing Node), assegura o acesso em tempo real aos dados cíclicos e apenas permite a comunicação de tramas TCP/IP (*non real time*) em *slots* de tempo reservadas para este tipo de dados. Todos os outros nós são os CNs (Controlled Nodes) e apenas podem enviar dados a pedido do MN.

O ciclo de comunicação de um sistema EPL é composto por quatro períodos: *Start*, *Isochronous*, *Asynchronous* e *Idle* (Figura 2.9) [18]. No período *Start* o MN envia uma trama *multicast* SoC (Start of Cycle), que indica o início do ciclo. No período *Isochronous* o MN envia uma trama *unicast* PReq (Poll Request) para cada um dos CNs e o CN acedido envia uma trama *multicast* PRes (Poll Response). No início do período *Asynchronous* o MN envia uma trama SoA (Start of Asynchronous) e o acesso ao meio é permitido tanto ao MN como a qualquer CN, mas apenas pode ser enviada uma trama ASnd (ASynchronous data). O protocolo tipicamente usado neste período é o UDP/IP. Desta forma a transmissão de dados assíncronos nunca interfere com a transmissão de dados síncronos, o que garante um *timing* preciso na comunicação.

Figura 2.9 - Ciclo de comunicação do EPL

TCnet

É uma proposta da Toshiba. Tal como no EPL, a *interface* TCnet está entre a camada física e a camada de ligação de dados. O acesso MAC (Medium Access Control) típico da Ethernet, o CSMA/CD, é modificado.

O período de transmissão de alta velocidade é composto por um serviço de transmissão de dados cíclico em tempo real (no TCnet utiliza-se a expressão *time critical*) e por um serviço de transmissão assíncrona (no TCnet é denominada como *sporadic*) (Figura 2.10) [18].

Cada período de transmissão de alta velocidade é iniciado com o *broadcast* de uma trama SYN para todos os nós da rede. Depois de receber a trama SYN, o nó 1 inicia a transmissão das suas tramas de dados (DT). Quando termina faz o *broadcast* de uma trama CMP, que indica o fim da sua transmissão. Esta é recebida pelo nó 2, que inicia a transmissão das suas tramas de dados, repetindo-se o processo até ao último nó.

Figura 2.10 - Ciclo de comunicação do TCnet

EPA

O protocolo EPA é uma proposta chinesa.

Este protocolo permite uma comunicação determinística baseada num mecanismo de divisão de tempo dentro da camada MAC. O *macrocycle* (T) é o tempo total para completar um procedimento de transmissão de dados. Esse tempo é dividido em duas fases: a fase para transmissão de mensagens periódicas (Tp) e a fase para transmissão de mensagens aperiódicas (Tn) (Figura 2.11) [18].

A última parte de cada mensagem periódica é um anúncio de mensagem não periódica, que indica se o dispositivo que enviou a mensagem periódica tem ou não uma mensagem não periódica para transmitir. Se tiver, o dispositivo só a poderá enviar na fase Tn.

Figura 2.11 - Ciclo de comunicação do EPA

PROFINET CBA

Foi definido por um conjunto de vários fabricantes, incluindo a Siemens, e é mantido pela PROFIBUS Internacional.

A primeira versão foi baseada no CBA (Component Based Automation) e está incluída no IEC 61784-1 (tipo 10 no IEC 61158).

Para a transmissão de dados sem requisitos de tempo real é utilizada a *stack* TCP/IP e protocolos como o RPC (Remote Procedure Call) e o DCOM (Distributed Component Object Model). Quando é necessária comunicação em tempo real (para ciclos de tempo abaixo dos 100 ms) não é utilizada a *stack* TCP/IP, sendo preferido o protocolo em tempo

real, que é baseado no *Ethertype* 0x8892 e no mecanismo de atribuição de prioridade à trama.

Modified Ethernet

A topologia da cablagem típica da Ethernet é a topologia em estrela: todos os componentes estão ligados a um dispositivo central de *switch*.

Nas aplicações da área da automação, com a introdução do *fieldbus* a topologia em estrela foi substituída por topologias em barramento ou em anel para reduzir os custos na cablagem.

As soluções RTE devem estar preparadas, tanto para as topologias utilizadas no chão de fábrica, como para a topologia da *swicthed Ethernet*. Para isso existem duas soluções: ou a infraestrutura da rede de campo tem um *switch* para cada dispositivo, ou a funcionalidade de *switch* é integrada nos próprios dispositivos da rede de campo.

SERCOS

O SERCOS III é uma extensão RTE do SERCOS, definido pelo *standard* IEC 61491 (Electrical Equipment of Industrial Machines – Serial Data for Real-Time Communication for Controls and Drives), o seu processo de standardização teve início em 2005 e culminou em 2007 com a aprovação do *standard* IEC 61784-2/61158.

No sistema SERCOS existe uma estação *master* e estações *slave*s, cujo número pode variar entre 1 e 254. Todas as estações têm duas portas Ethernet. A topologia da rede pode ser *daisy-chain* ou em anel. Não são permitidos *switches* entre estações e, apenas no caso da topologia *daisy chain*, a porta Ethernet livre do último *slave* pode ser ligada a um *switch*, se for requerida comunicação entre dispositivos via TCP/IP ou UDP/UDP.

No sistema SERCOS III o ciclo de comunicação está dividido em dois períodos, denominados de canais de comunicação: o primeiro é o canal *real time* e o segundo, com menor duração, é o canal *non real time* (Figura 2.12) [18].

O ciclo de comunicação é iniciado pelo *master*, que envia a t*odos os slaves* dois tipos de telegramas *real time*: até 4 MDTs (Master Data Telegrams) e até 4 ATs (Answer Telegrams). Os MDTs contêm informação para sincronização, informação de controlo, dados de serviço do canal e valores de comando. Os ATs são transmitidos pelo *master* como uma trama vazia, mas com campos pré definidos, sendo cada um desses campos destinado a um determinado *slave*. Se um *slave* pretende enviar informação coloca-a no

seu campo e envia o telegrama AT. Quando termina o canal *real time* é iniciado o canal *non real time*, durante o qual podem ser enviados telegramas *non real time*.

Figura 2.12 - Ciclo de comunicação do SERCOS III

ETHERCAT

Este protocolo foi definido pela Beckoff e é mantido pelo grupo de tecnologia Ethercat (ETG). Utiliza as tramas Ethernet e uma topologia em anel especial.

Utiliza um mecanismo de acesso ao meio do tipo *master-slave*, no qual o nó *master* (tipicamente o sistema de controlo) envia tramas *Ethernet standards* ISO/IEC 8802-3 para os nós *slaves*, que por sua vez recebem e enviam dados através dessas tramas.

PROFINET IO

Este protocolo foi definido por vários fabricantes, sendo o mais importante a Siemens, e é mantido pela PROFIBUS Internacional.

Depois da definição PROFINET CBA, o passo seguinte foi a definição de um modelo de aplicação para o PROFINET IO baseado no PROFIBUS DP (tipo 3 do IEC 61158).

Num sistema deste tipo existem três tipos de dispositivos: os controladores IO, os dispositivos IO e o supervisor IO. Os controladores IO controlam os dispositivos IO com comunicação de dados cíclica através de um *buffer*. O supervisor IO gere o funcionamento dos componentes IO e dos controladores IO do sistema.

O ciclo de troca de dados entre os componentes de um sistema PROFINET IO é dividido nas seguintes fases de comunicação: IRT (Isochronous Real Time), RT (Real Time) e NRT (Non Real Time) (Figura 2.13) [18].

Na fase *Isochronous* a comunicação é escalonada no tempo: em cada tempo de offset a trama IRT é enviada de uma porta para outra sem interpretação do endereço por parte do switch. Nas fases seguintes os *switches* comportam-se como *switches standard* Ethernet, passando a comunicação a ser baseada no endereço. Primeiro são transmitidas as tramas RT durante a fase RT e quando esta termina é iniciada a fase NRT, durante a qual são transmitidas as tramas NRT.

Figura 2.13 - Ciclo de comunicação do PROFINET IO

2.7 Conclusão

Neste capítulo foram abordadas as redes de comunicação industriais, tendo sido feita uma análise aos principais protocolos actualmente utilizados.

Pode-se questionar sobre a necessidade do desenvolvimento de tantos protocolos. No entanto, tal facto é justificado, por um lado, pela pressão dos vários grupos económicos e, por outro, pela complexidade e variedade das possíveis áreas de aplicação.

Em relação a este segundo aspecto, é de facto difícil de conceber que uma única norma consiga abranger todas as áreas de aplicação e, nas várias tentativas feitas, provou-se que tal norma se tornava demasiado complexa, tendo um custo de implementação demasiado alto.

Quanto ao primeiro ponto, é evidente que as empresas fabricantes de sistemas e equipamento não tinham, e não têm, interesse em divulgar os protocolos de comunicação, para proteger os investimentos feitos em termos de I&D (Investigação e Desenvolvimento).

No entanto, depois de muitos anos de esforços foi adoptada uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 e o IEC 61784, que englobam as soluções comerciais mais importantes, incluindo soluções RTE.

Compete ao utilizador final e ao mercado decidir quais das soluções propostas preenchem os requisitos das aplicações em automação.

2 Redes de Comunicações Industriais

2.1 Introdução

A evolução da tecnologia nos últimos anos teve uma grande influência na sociedade, levando a caracterizá-la hoje como a sociedade do conhecimento. Com efeito, a globalização é hoje uma realidade, permitindo um rápido acesso à informação onde quer que ela se encontre, originando assim um esforço de actualização constante, já que a informação de que hoje dispomos ficará rapidamente ultrapassada.

O reflexo nas empresas fabris desta maneira de estar da sociedade actual traduz-se em novos desafios, no que respeita à produtividade: o nível de exigência do consumidor aumentou, os ciclos de vida dos produtos diminuíram, as linhas de produção tiveram de ser optimizadas em termos de níveis de *stocks* e flexibilidade, tudo a um baixo custo, para ser possível responder às necessidades do mercado de uma forma rentável. Este desafio nas áreas da inovação e da competitividade obrigou as empresas a concentrar esforços na modernização tecnológica dos seus processos de fabrico, nomeadamente na automatização dos mesmos. Deste esforço integrado resultaram, para além de produtos mais competitivos, o desenvolvimento de soluções tecnológicas avançadas que, à medida que se tornaram cada vez mais comuns e acessíveis, passaram também a ser incorporadas nos próprios processos de fabrico.

Durante as últimas três décadas assistiu-se a uma evolução sem paralelo na área dos sistemas de controlo, nomeadamente ao nível dos respectivos processos de concepção, implementação e operação. Isto deveu-se, em grande parte, aos novos desenvolvimentos, quer em áreas tecnológicas, tais como a microelectrónica e as telecomunicações, quer em áreas associadas à gestão e à integração de sistemas, bem como ao desejo de disponibilizar aos utilizadores finais equipamentos com maiores funcionalidades a custos mais reduzidos.

Este desenvolvimento reflectiu-se também ao nível das comunicações industriais, através da substituição progressiva das tradicionais comunicações ponto-a-ponto pelas

LANs (*Local Area Networks*). Embora inicialmente os motivos desta mudança estivessem relacionados com aspectos económicos, tais como a redução da cablagem e dos custos de manutenção, resultaram posteriormente em enormes vantagens ao nível da descentralização do controlo dos processos, na facilidade de instalação e configuração, na elevada flexibilidade de utilização e na melhoria do desempenho dos sistemas de controlo.

A crescente descentralização ao nível das funções de controlo e a crescente utilização de dispositivos inteligentes baseados em microprocessadores ou microcontroladores, criaram as condições necessárias para o desenvolvimento e proliferação das redes de campo. Estas são um tipo específico de rede local industrial, com o objectivo de interligar controladores, sensores e actuadores, que realizam a *interface* com o processo industrial.

Neste capítulo são analisadas as redes de comunicações industriais, com destaque para as redes de campo, os seus *standards* e as soluções comerciais ao nível das redes com fios. Neste contexto, na secção 1.2 é abordado o sistema de controlo do ambiente industrial, sendo ainda feito um resumo sobre a evolução das tecnologias de controlo. Na secção 1.3 é feita uma descrição do modelo OSI, uma vez que os *standards* de redes de campo são baseados nesse modelo. De seguida, na secção 1.4 é analisada a arquitectura das comunicações industriais, sendo ainda estabelecida uma relação entre esta e os níveis de controlo existentes num ambiente industrial. Na secção 1.5 são abordadas as redes de campo em particular, é feito um breve resumo sobre a história da standardização deste tipo de redes e são ainda apresentados os protocolos incluídos no conjunto de *standards* que especificam este tipo de redes. Por último, na secção 1.6 é abordada a *Ethernet* em tempo real e são apresentadas as soluções RTE (Real Time Ethernet) existentes.

2.2 O Sistema de controlo

O funcionamento de forma correcta e segura de um processo industrial de qualquer natureza é assegurado por intermédio de um sistema de controlo apropriado. Independentemente da dimensão ou da complexidade do processo em causa, o respectivo sistema de controlo pode ser decomposto em três subsistemas com funções bem definidas: o processo controlado, o controlador e o operador humano (Figura 2.1) [5].

Figura 2.1 - Sistema de controlo

O controlador é um equipamento que interage com o seu ambiente através de duas *interfaces* com características distintas:

- a *interface* com o processo controlado é definida como a *interface* de instrumentação;
- a *interface* com o operador humano é definida como a *interface* homem-máquina.
- A *interface* de instrumentação consiste num conjunto de sensores e actuadores que transformam os sinais físicos do processo controlado em sinais com características apropriadas para serem utilizados pelo controlador, e vice-versa. A *interface* homem-máquina consiste num conjunto de dispositivos de entrada e saída, que permitem a interacção com um operador humano. Tipicamente, esta interacção realiza-se ao nível da definição de parâmetros do processo e da supervisão da respectiva evolução.

A função do controlador é controlar a evolução do processo através da execução de um algoritmo de controlo adequado. A partir do processamento da informação obtida, quer directamente do estado do processo através da *interface* de instrumentação, quer fornecida pelo operador humano através da *interface* homem-máquina, o algoritmo de controlo produz um conjunto de comandos que são enviados para o processo através da *interface* de instrumentação. Para realizar estas funções o controlador dispõe de uma estrutura funcional, baseada na utilização de equipamentos adequados ao processo em causa, que suporta a execução do algoritmo de controlo.

Ao nível da estrutura funcional, estes sistemas de controlo podem ser classificados em três tipos de arquitecturas (Figura 2.2) [5].

- Centralizadas - o algoritmo de controlo é executado por um único equipamento;
- Descentralizadas - o algoritmo é executado num único equipamento, mas

algumas tarefas de processamento mais simples (ex. condicionamento e aquisição de sinais) são executadas por outros equipamentos de menor complexidade. Isto implica a existência de uma estrutura de comunicações que permita a interacção e a cooperação entre os vários equipamentos (ex. comunicações série ponto-a-ponto);

- Distribuídas - o algoritmo de controlo encontra-se distribuído por vários equipamentos de complexidade e natureza distintas. Tal como nas arquitecturas descentralizadas, é também necessário dispor de uma estrutura de comunicações adequada, sendo esta, contudo, comparativamente muito mais complexa (ex. rede de campo).

Figura 2.2 - Exemplos de arquitecturas de controlo

2.2.1 Evolução das Tecnologias de Controlo

O advento do computador no início dos anos 60 permitiu que estes passassem também a ser utilizados para implementar funções de controlo. O termo DCC (Direct Digital Control) foi utilizado na época para enfatizar o facto do controlo do processo ser realizado directamente pelo computador. O facto de serem programáveis proporcionou-lhes uma esmagadora vantagem em comparação com as tecnologias de lógica discreta utilizadas até ao momento. Um único equipamento (um computador) concentra em si, quer

as tarefas do controlador, quer as *interfaces* de instrumentação e de homem-máquina. No caso da *interface* de instrumentação, os sensores e actuadores são tipicamente ligados ao controlador através de ligações ponto-a-ponto analógicas (ex. anel de corrente). Em paralelo com este processo, tem também início nos finais do anos 60 o desenvolvimento de máquinas de controlo numérico e de *robots* industriais.

As arquitecturas de controlo desenvolvidas até esta época são essencialmente centralizadas. Contudo, as crescentes exigências da indústria, conjugadas com o desenvolvimento do microprocessador no início dos anos 70, permitiram uma evolução para as primeiras arquitecturas descentralizadas. Esta evolução efectuou-se segundo duas perspectivas [6]:

- uma ao nível das indústrias de processos, com o desenvolvimento dos DCS (Distributed Control Systems) com o objectivo de interligar hierarquicamente os equipamentos de controlo de menor complexidade (por exemplo controladores PID - Proportional Integral Derivative) aos equipamentos de maior complexidade (por exemplo mini-computadores);
- outra ao nível das indústrias de manufactura, onde o PLC, cujo desenvolvimento se deu no início dos anos 70, foi utilizado como elemento central das arquitecturas de controlo.

Em ambas as perspectivas, a interligação entre equipamentos era tipicamente realizada, quer através de ligações ponto-a-ponto analógicas, quer através de ligações digitais, utilizando neste último caso protocolos de comunicação proprietários. Embora esta evolução tenha permitido o desenvolvimento de sistemas de controlo cada vez mais complexos, durante a primeira década da sua utilização, as arquitecturas de controlo continuaram a ser caracterizadas por uma estrutura tipicamente centralizada e só mais tarde se registou uma evolução para soluções do tipo descentralizado.

Entre meados dos anos 80 e inícios dos 90, assistiu-se a uma alteração da estrutura das arquitecturas de controlo através da crescente utilização de redes de comunicação industriais para interligar os equipamentos de controlo. Esta evolução tecnológica foi o ponto de partida das primeiras arquitecturas de controlo descentralizadas baseadas numa estrutura de comunicações digital. Estas arquitecturas, embora mais complexas, permitiram obter um importante conjunto de vantagens, das quais se destacam: menores custos, melhores desempenhos, instalação e manutenção mais simples, modularidade, facilidade

na detecção de erros e avarias, etc. Na sequência desta evolução, surge também nesta época o conceito de CIM (Computer Integrated Manufacturing).

O CIM visa a cooperação entre os diferentes sistemas intervenientes no ambiente de fabrico e engloba todas as actividades com ele relacionadas, desde o projecto e desenvolvimento até ao *marketing* e vendas, passando pelo controlo do fabrico. Para que essa cooperação exista de facto é necessário que haja integração entre os sistemas. A integração significa a possibilidade de os subsistemas da empresa poderem interactuar entre si através de sistemas de comunicações de dados e bases de dados comuns.

Os sistemas de comunicações requerem infraestruturas técnicas (*software* e *hardware*). As comunicações requerem também regras (protocolos), regras essas condicionadas, não apenas por aspectos técnicos, mas também pela funcionalidade exigida.

Uma das representações da filosofia CIM consiste em decompor a empresa em cinco níveis, tal como a figura 2.3 indica.

Figura 2.3 - Representação da filosofia CIM

A subdivisão em níveis é baseada, entre outros aspectos, nos tipos de actividades realizadas na empresa e leva, geralmente, ao uso de diferentes tipos de redes de comunicações nos vários níveis.

No interior de cada nível as comunicações horizontais são geralmente asseguradas por uma rede local. As comunicações verticais entre dois níveis adjacentes são resolvidas interligando as redes através de dispositivos de ligação.

A figura 2.4 representa um exemplo de uma arquitectura possível para a hierarquia de comunicações dentro de uma empresa.

Nos níveis superiores da hierarquia as comunicações podem ser caracterizadas como correspondendo à troca de grandes quantidades de informação, que tem de ser processada durante períodos relativamente longos mas com uma frequência relativamente baixa.

Ao contrário, nos níveis inferiores da hierarquia pequenas quantidades de informação precisam de ser processadas de uma forma rápida, com o objectivo de controlar processos industriais em tempo real. Este tipo de transacções tem normalmente uma periodicidade cíclica e uma frequência relativamente elevada.

Pode-se então concluir que não é possível satisfazer todos estes requisitos de transferência de dados com um só tipo de rede.

Figura 2.4 - Representação de uma arquitectura possível para a hierarquia das comunicações de uma empresa

Pode assim propor-se uma classificação hierárquica das comunicações industriais em três grandes grupos, que são: redes de fábrica, redes de célula e redes de campo.

As redes de fábrica abrangem os níveis superiores da hierarquia, enquanto as redes de campo correspondem ao nível mais baixo.

Embora esta evolução abrisse um conjunto enorme de perspectivas ao nível da integração de equipamentos situados em diferentes níveis de controlo, na prática isto acabou por não se verificar, devido ao desenvolvimento de muitas soluções proprietárias. Estas acabaram por limitar as potencialidades das arquitecturas de controlo, nomeadamente

ao nível da integração e da interoperabilidade entre equipamentos. Este problema colocou-se de forma especialmente grave ao nível das redes de campo, com os diferentes fabricantes a tentar impor as suas soluções como o *standard* a utilizar. São alguns exemplos o (PROcess FIeld BUS), o WorldFIP (Factory Instrumentation Protocol), o DeviceNet, o INTERBUS-S, e o AS-Interface (Application Server). Este processo terminou apenas recentemente através da adopção de uma solução de compromisso entre as várias propostas existentes [7]. Ao nível das arquitecturas de controlo registou-se uma tendência para adoptar soluções distribuídas, não só devido à possibilidade de dispor de equipamentos com maiores capacidades de processamento, mas também através do desenvolvimento de arquitecturas de comunicação que suportam elevados níveis de integração entre equipamentos.

Embora a introdução das redes industriais viesse resolver o problema da integração horizontal de equipamentos (situados no mesmo nível de controlo), a integração vertical (entre níveis de controlo) foi sempre um problema em aberto. As soluções apontadas inicialmente passavam pela utilização de equipamentos dedicados (*gateways*) ou pelo desenvolvimento de *software* específico que implementava as tarefas de mapear os serviços de comunicação das diferentes redes. Como estas soluções eram normalmente caras e complexas, surgiu no final dos anos 80 a ideia de desenvolver uma arquitectura de comunicações aberta baseada na estrutura do modelo OSI (*Open Systems Interconnection*). Exemplos destas soluções foram o MAP (Manufacturing Automation Protocol) e o MMS (Manufacturing Message Specification). No entanto, o seu sucesso acabou por ser limitado devido, quer à falta de suporte tecnológico adequado, quer à cumplicidade das soluções propostas.

Em paralelo, nas indústrias de processos a utilização de tecnologias SCADA (Supervisory Control and Data Aquisition) foi vista como uma alternativa mais simples e razoavelmente eficaz na integração vertical. Contudo, devido, quer à ausência de adequação destes sistemas para o problema em causa, quer à proliferação de equipamentos de controlo com características muito diversas, a utilização desta tecnologia acabou por resultar em soluções bastante limitadas.

Nos finais dos anos 90, devido às crescentes exigências de integração com aplicações de nível intermédio e superior, nomeadamente o ERP (Enterprise Resource Planning) e o MES (Manufacturing Execution System), foram desenvolvidas um conjunto de tecnologias de *software* baseadas em plataformas de objectos distribuídos, que disponibilizavam uma

infraestrutura ao nível dos serviços de comunicações, permitindo assim desenvolver de forma eficaz os conceitos de integração vertical e horizontal. São exemplos destas tecnologias o CORBA (Common Object Request Broker Architecture), com uma gama alargada de domínios de aplicação, e o OPC (Object linking and embedding for Process Control), que foi especialmente desenvolvido para satisfazer os requisitos no domínio das aplicações industriais. Este processo apresenta actualmente uma grande dinâmica, com destaque para o desenvolvimento de *standards* com base em arquitecturas de objectos distribuídos especialmente vocacionados para as necessidades dos ambientes industriais: IEC 61499 (Function Blocks for Industrial-Process Measurement and Control Systems) e o IEC 61804 (Function Blocks for Process Control). Como resultado deste trabalho, as arquitecturas de comunicação mais recentes já incorporam muitas destas funcionalidades, das quais se destacam: o CIP (Common Industrial Protocol), o IDA (Interface for Distributed Automation), o HSE *fieldbus* (High Speed Ethernet) e o PROFINET.

Entre os finais dos anos 90 e o início da corrente década verificou-se um fenómeno de migração de tecnologias de uso geral para a área das comunicações industriais. O caso mais paradigmático deu-se com a utilização da rede Ethernet em ambientes industriais (IE - Industrial Ethernet). Este processo teve um profundo impacto na estrutura das comunicações industriais, afectando todos os níveis de controlo. Esta migração deveu-se a vários factores, tais como: a existência de soluções de *hardware* de baixo custo e de elevado desempenho, bem como de protocolos de comunicação abertos e a disponibilização de plataformas de *software* para o desenvolvimento integrado de aplicações distribuídas.

A etapa mais recente desta evolução está centrada na utilização das tecnologias desenvolvidas para Web, tais como UDP/TCP/IP (User Datagram Protocol / Transmission Control Protocol / Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), XML (eXtensible Markup Language), Proxys, Java, ou Jini, para o desenvolvimento de aplicações industriais. A utilização destas tecnologias, para além de estarem largamente difundidas e do seu custo reduzido, vai permitir obter níveis de integração superiores nomeadamente ao nível dos domínios de aplicação externos ao ambiente industrial [11].

Associado ainda a este processo de migração de tecnologias emergentes para as redes industriais, é de salientar a crescente tendência para a utilização de redes de comunicações sem fios (como o IEEE 802.11 ou o IEEE 802.15) em ambientes industriais [9], [10].

2.3 O Modelo de Referência OSI

Convém agora, fazer uma descrição do modelo OSI, uma vez que os protocolos de comunicações industriais a seguir mencionados têm como referência esse modelo.

Num ambiente onde existem equipamentos provenientes de diferentes fabricantes a integração implica a definição de protocolos de comunicação normalizados. A ISO (International Organization for Standardization) definiu o modelo de referência OSI com o objectivo de promover o aparecimento de normas na área das comunicações entre computadores, equivalente ao que na altura se verificava já para as comunicações telefónicas, definidas no âmbito da CCITT (Commité Consultatif International de Telegraphique et Telephonique) [12]. O termo “sistema de arquitectura aberta” indica que se um sistema estiver conforme com o modelo OSI então está aberto a comunicar com qualquer outro que obedeça às mesmas normas. É de salientar que o modelo de referência OSI não especifica por si as normas de comunicação. O seu propósito é apenas fornecer uma arquitectura que sirva de base ao desenvolvimento de normas para sistemas de comunicação.

O modelo de referência OSI define 7 camadas, conforme se indica na figura 2.5.

Figura 2.5 - O modelo de referência OSI

A hierarquia dos níveis vai subindo, desde o nível de maior especificidade até ao mais alto, que é o nível mais genérico.

Os três primeiros níveis fornecem um serviço de rede, ou seja, tratam do transporte da informação. O nível físico trata do meio físico para a transmissão de *bits* de informação, o nível lógico organiza os *bits* de uma forma ordenada em blocos (tramas) e assegura que eles são transmitidos e recebidos de uma forma correcta, enquanto o nível de rede assegura que os pacotes chegam ao seu destino final.

Enquanto o serviço de rede fornecido pelos três níveis inferiores é adequado para transportar informação, algumas aplicações podem ter especificações que as redes não fornecem, como por exemplo uma taxa de erros baixa, um elevado nível de segurança, ou a necessidade de manter uma sequência de pacotes que façam uma mensagem completa. São estes os serviços que o nível de transporte fornece aos níveis superiores.

Os níveis acima do nível de transporte não tratam de mecanismos de transmissão de informação. Esse é o trabalho dos quatro níveis inferiores. No entanto, a informação necessita de ser sincronizada e tratada para que as aplicações entendam. O nível de sessão fornece o serviço de gestão da comunicação entre aplicações.

Outro ponto importante é o formato em que a informação é trocada. Os dois sistemas que estão a comunicar podem ter maneiras diferentes de representar os dados. O nível de apresentação preenche o requisito de identificar e estabelecer uma sintaxe comum, que será utilizada pelos dois sistemas.

O nível mais alto é o nível de aplicação, que constitui a *interface* entre as aplicações propriamente ditas e o sistema de comunicações.

Tendo sido feita uma introdução do modelo, a seguir é feita uma abordagem mais detalhada, especificando, em cada nível: os seus objectivos, os serviços oferecidos ao nível imediatamente superior e as suas funções.

2.3.1 O Nível Físico

O nível físico é responsável por uma transmissão transparente da informação através do meio físico. As funções do nível físico são inteiramente independentes do meio físico em uso, seja este constituído por fio de cobre, cabo coaxial ou fibra óptica. O tipo de meio físico utilizado é completamente escondido ao nível lógico pelo nível físico.

As definições do nível físico podem ser agrupadas da seguinte forma:

- Mecânicas: definem o tipo de conector, as dimensões físicas, as posições dos

pinos, etc;

- Eléctricas: definem as características eléctricas, como por exemplo: níveis eléctricos, impedância, etc;
- Funcionais: definem qual o significado dos níveis eléctricos em determinados pinos do conector;
- Procedimentais: definem as regras (procedimentos) a aplicar às várias funções e também qual a sequência em que determinados eventos podem ocorrer.

Serviços Fornecidos ao Nível Lógico

O nível físico fornece os seguintes serviços ao nível lógico:

- Ligações físicas: o fornecimento de uma transmissão de *bits* perfeitamente transparente entre entidades lógicas. A ligação física estabelece um “circuito de informação” entre dois pontos. A ligação física pode ser estabelecida entre dois pontos ou directamente, ou através de um sistema intermédio;
- Tratamento das unidades de informação: este serviço compreende a transmissão de um *bit* em transmissão série, ou de n *bits* em transmissão paralela. A ligação física pode ser *full-duplex* (a informação é feita nos dois sentidos simultaneamente), *half-duplex* (a informação é feita nos dois sentidos mas alternadamente), ou ainda *simplex* (a informação só é feita num sentido);
- Ligação entre pontos: a ligação entre pontos pode ser ponto-a-ponto ou multiponto;
- Sequenciamento: o nível físico coloca os *bits* no meio físico na mesma ordem que lhe foram fornecidos pelo nível lógico
- Identificação de circuito: o nível físico fornece identificadores que definem univocamente a ligação entre dois sistemas. O nível físico fornece identificadores da ligação entre pontos, que podem ser utilizados pelo nível lógico;
- Recuperação de falhas: o nível lógico é notificado de problemas detectados pelo nível físico;
- Parâmetros fornecidos ao nível lógico: são fornecidos parâmetros ao nível lógico, tais como: taxas de erro, taxas de transmissão, disponibilidade de serviço e atrasos.

Funções do Nível Físico

As seguintes funções são executadas pelo nível físico:

- Estabelecimento e libertação das ligações entre entidades do nível lógico;
- Transmissão de sequências de *bits*: estas podem ser síncronas ou assíncronas;
- Gestão: os protocolos do nível físico tratam de alguns aspectos relacionados com a gestão das actividades deste nível.

2.3.2 O Nível Lógico

O nível lógico isola os níveis superiores das características do meio de transmissão e fornece uma ligação sem erros e de confiança. O nível lógico é estabelecido sobre uma ou mais redes físicas e liga duas identidades em sistemas adjacentes. As ligações lógicas são ponto-a-ponto.

Dentro do nível lógico as sequências de *bits* do nível físico são organizadas em blocos de informação denominados tramas. São funções do nível lógico a sincronização dos *bits* dentro de uma trama, a detecção e correcção de erro (através da retransmissão de pacotes) e ainda o controlo de fluxo (dependendo do estado do sistema de recepção, liga ou desliga a transmissão de pacotes).

Serviços Fornecidos ao Nível de Rede

Os seguintes serviços são fornecidos pelo nível lógico:

- Ligação lógica: o estabelecimento de uma ou mais ligações entre duas entidades;
- Unidades de informação do nível lógico: estas entidades teóricas são mapeadas numa base de uma para uma em unidades do protocolo em uso. Na prática, estas são as tramas transmitidas numa ligação lógica;
- Identificadores lógicos: se requerido pelo nível físico, o nível lógico pode fornecer identificadores dos pontos da ligação lógica;
- Sequenciamento: manutenção da sequência correcta de pacotes;
- Detecção de erros: se for detectado um erro não recuperável pelo nível lógico, então o nível físico será notificado;
- Controlo de Fluxo: o nível de rede pode controlar dinamicamente a taxa a que pode receber os pacotes;
- Parâmetros da qualidade do serviço: estes parâmetros são opcionais e incluem

tempos médios entre erros detectados mas irrecuperáveis, taxa de erro residual, disponibilidade do serviço e débito.

Funções do Nível Lógico

As seguintes funções são efectuadas no nível lógico:

- Estabelecimento e libertação das ligações do nível lógico: como foi referido, esta função faz um mapeamento das unidades de informação em unidades do protocolo, em uso numa forma de uma para uma;
- Separação de ligações lógicas: esta função é feita dividindo uma ligação lógica em várias ligações físicas;
- Delimitação e sincronização: esta é essencialmente uma função de empacotamento, que organiza *bits* (unidades do nível físico) em tramas (unidades lógicas);
- Controlo de sequência: mantém a ordem sequencial dos pacotes transmitidos através da ligação lógica;
- Detecção de erros: esta função detecta erros de transmissão, de formato e de operação, que usualmente aparecem devido a deficiências no meio físico;
- Recuperação de erros: esta função tenta recuperar os erros, geralmente através da retransmissão de pacotes;
- Controlo de fluxo: fornece os serviços de controlo de fluxo já descritos;
- Identificação e troca de parâmetros: efectua a identificação de entidades lógicas e controla a troca de parâmetros;
- Controlo da ligação do circuito de dados: esta função fornece o nível de rede com a informação necessária para controlar e manter o circuito de dados ao nível de rede;
- Gestão: os protocolos do nível físico tratam de alguns aspectos da gestão das actividades deste nível.

2.3.3 O Nível de Rede

A função essencial do nível de rede é fornecer uma transmissão de dados perfeitamente transparente de um nível de transporte de um sistema (por exemplo uma aplicação num terminal) a um nível de transporte de outro sistema (por exemplo a aplicação servidora num computador central).

Em redes complexas, entidades comunicantes no nível de transporte não necessitam de estar próximas, mas ligadas através de um ou mais sistemas intermédios. Nestes casos, o nível de rede fornece funções de encaminhamento. Um exemplo pode ser a ligação de uma rede pública de dados com uma rede privada (por exemplo uma rede bancária) e uma rede local. Os endereços de rede são utilizados para identificar as várias entidades comunicantes no nível de transporte ao nível de rede.

Serviços Fornecidos ao Nível de Transporte

Os seguintes serviços são fornecidos pelo nível de rede:

- Endereços de rede: são fornecidos pelo nível de rede e são usados por entidades do nível de transporte, de forma a identificar univocamente outras entidades do nível de transporte;
- Ligações de rede: fornecem os meios de transferir dados entre entidades do nível de transporte;
- Identificadores de Ligações Rede entre sistemas: o nível de rede fornece às entidades do nível de transporte um identificador de ligação associado univocamente com o endereço de rede;
- Unidades de informação do nível de rede: numa ligação de rede o nível de rede fornece, para transmissão, unidades de informação (pacotes de dados). Estas unidades têm um cabeçalho e um final perfeitamente definidos. A integridade da unidade é verificada no nível de rede;
- Parâmetros de qualidade do serviço: estes parâmetros incluem taxa residual de erros, disponibilidade do serviço, habilidade, débito, atraso no tráfego e atraso no estabelecimento de ligações na rede;
- Notificação de erros: erros irrecuperáveis para o nível de rede são participados ao nível de transporte;
- Sequenciamento: o nível de rede pode fazer a entrega de unidades de informação do nível de rede sequencialmente para uma determinada ligação de rede;
- Controlo de fluxo: a entidade de transporte que está a receber pode fazer com que o Serviço de Rede pare de enviar mais unidades de informação. Este controlo de fluxo pode ou não ser enviado ao outro extremo da ligação;
- Libertação: a entidade de transporte pode pedir a libertação da ligação.

Funções do Nível de Rede

As funções de nível de rede fornecem uma grande variedade de configurações, desde ligações ponto-a-ponto a ligações mais complexas, com uma combinação de várias sub-redes. As seguintes funções são efectuadas:

- Encaminhamento e repetição: as ligações da rede são fornecidas por entidades nos sistemas finais, mas podem ser envolvidas entidades em sistemas intermédios que façam repetição. As funções de encaminhamento determinam um caminho definido entre dois endereços;
- Ligações de rede: esta função fornece ligações entre entidades do nível de transporte, fazendo uso de ligações fornecidas pelo nível lógico;
- Multiplexação de ligações de rede: esta função é usada para multiplexar ligações de rede em ligações lógicas;
- Segmentação e empacotamento: o nível de rede pode segmentar e/ou formar blocos que constituem unidades de informação do nível de rede, para facilitar o transporte;
- Funções de detecção de erros: são utilizadas para verificar se a qualidade dos serviços fornecidos numa rede é mantida. Quando há detecção de erros no nível de rede o nível lógico é notificado. As funções de recuperação de erros dependem da qualidade do Serviço de Rede fornecido;
- Sequenciamento: prevê a entrega sequencial de unidades de informação do Serviço de Rede numa determinada ligação;
- Controlo de fluxo;
- Selecção de serviços: esta função permite que sejam seleccionadas as mesmas funções nos dois sistemas, mesmo quando a ligação se faz entre vários subsistemas.

2.3.4 O Nível de Transporte

O papel do nível de transporte é complementar a rede que está por baixo, de forma a assegurar a qualidade dos serviços requeridos que estão acessíveis ao utilizador.

As funções do nível de transporte estão focalizadas em optimização de custos, controlo de erros, controlo de fluxos, sequenciamento e multiplexagem. O nível de transporte também verifica a existência de duplicados e perdas de informação. Se a ligação de rede for quebrada temporariamente, a ligação de transporte pode ser mantida até que a ligação seja restaurada.

Os protocolos do nível de Transporte são definidos para aceitar uma grande variedade de redes, com várias qualidades de serviços. São cinco as classes de Serviços de Transporte disponíveis:

- A classe 0 é a classe mais simples, sem melhoramentos nos Serviços de Rede;
- A classe 1 adiciona recuperação de erros para redes sujeitas a uma grande frequência de interrupções;
- A classe 2 tem as funções da classe 0 mais multiplexagem;
- A classe 3 tem as funções da classe 1 mais multiplexagem;
- A classe 4 adiciona funções de detecção de erros e de dados fora de sequência.

Serviços Fornecidos ao Nível de Sessão

Os seguintes serviços são fornecidos pelo nível de transporte:

- Estabelecimento de ligações de transporte: as ligações de transporte são estabelecidas entre identidades do nível de sessão e são identificadas pelo endereço de transporte. A qualidade do serviço é negociada entre as entidades do nível de sessão e o serviço de transporte;
- Transferência de dados: fornece a transferência de dados, de acordo com a qualidade de serviço que foi negociada;
- Libertação da ligação de transporte: fornece meios para que qualquer entidade da camada de sessão dos sistemas possa libertar a ligação de transporte.

Funções do Nível de Transporte

As operações no nível de transporte são:

1 Fase de Iniciação

Durante esta fase são efectuadas as seguintes funções:

- Obtenção de uma ligação à rede que corresponda aos requisitos em termos de custos e qualidade de serviço.
- Decisão de multiplexagem ou divisão.
- Estabelecer as unidades de informação do protocolo de transporte óptimas.
- Selecção das funções que devem estar operacionais durante a transferência de dados.
- Mapeamento dos endereços de transporte em endereços de rede.

- Fornecimento de identidade aos endereços de transporte.
- Transferência dos dados.

2 Fase de Transferência

Durante esta fase é executada a transmissão de unidades de informação do protocolo de transporte. Os seguintes serviços podem ser usados ou não, dependendo da classe de serviço seleccionada:

- Sequenciamento;
- Empacotamento;
- Segmentação;
- Multiplexagem ou divisão;
- Controlo de fluxo;
- Detecção e recuperação de erros;
- Transferência dos dados enviados;
- Delimitação das unidades de informação do serviço de transporte;
- Identificação das ligações de transporte.

3 Fase de Libertação

Esta fase inclui as seguintes funções:

- Notificação das razões da libertação.
- Identificação da ligação de transporte libertada.
- Transferência de dados.

2.3.5 O Nível de Sessão

Os requisitos para o nível de sessão reflectem a observação da utilização dos sistemas, pela maior parte dos utilizadores, em picos de actividade que podem ser chamados de sessões. Durante a sessão, o utilizador e o sistema iniciam um diálogo. A primeira função do nível de sessão é estabelecer, manter e gerir este diálogo.

As ligações da camada de Sessão são mapeadas em ligações da camada de transporte numa razão de um para um. Não existe multiplexagem neste nível, mas é possível que várias ligações de sessão usem a mesma ligação de transporte sequencialmente. Simultaneamente, uma ligação de sessão pode usar mais que uma ligação de transporte. Se a ligação de transporte se quebrar, devido a problemas nas camadas inferiores da rede, é possível estabelecer uma nova ligação de transporte sem a intervenção do utilizador ou

mesmo chegar ao seu conhecimento a quebra. Neste caso é o nível de sessão que é o responsável pela ressincronização do diálogo entre os dois sistemas.

Serviços Fornecidos ao Nível de Apresentação

Os seguintes serviços são fornecidos pelo nível de sessão:

- Estabelecimento da ligação entre níveis de sessão: permite que duas entidades do nível de apresentação possam estabelecer uma ligação de sessão entre elas;
- Libertação de ligação: permite que entidades do nível de apresentação possam libertar uma ligação do nível de sessão de uma forma ordeira e sem perda de informação;
- Transferência de dados: permite que uma entidade emissora do nível de apresentação possa transferir uma unidade de informação do nível de sessão a uma entidade receptora do nível de apresentação;
- Serviço de Quarentena: permite à entidade emissora solicitar que algumas unidades de informação, enviadas por uma conexão do nível de sessão, não devam ser enviadas à entidade receptora do nível de apresentação, até ordem contrária enviada pelo emissor;
- Gestão de Interacção: permite que entidades do nível de apresentação comandem explicitamente quem vai controlar certas funções de controlo. São possíveis os seguintes tipos de interacção: dois sentidos simultaneamente, dois sentidos alternadamente, um sentido;
- Sincronização de ligação: este serviço permite que entidades do nível de apresentação definam e identifiquem pontos de sincronização que obriguem uma ligação do nível de sessão a permanecer num determinado estado (*reset*) e que definam qual o ponto de ressincronização;
- Situações excepcionais: faz a notificação ao nível superior de quaisquer situações não englobadas pelos serviços deste nível.

Funções do Nível de Sessão

A maior parte das funções necessárias neste nível estão implícitas aos serviços deste nível:

- Mapeamento das ligações de sessão às ligações de transporte;
- Controlo do fluxo do nível de sessão: o nível de sessão não possui controlo de fluxo. Para evitar aumentar as funções do nível de sessão este controlo é feito no nível de

transporte;

- Recuperação de ligações quebradas: no caso de quebra de ligação do nível de transporte o nível de sessão pode ter as funções necessárias para restabelecer uma nova ligação, de forma a continuar a sessão;
- Libertação da ligação de Sessão: permite que se acabe e liberte a ligação sem perda de informação.

2.3.6 O Nível de Apresentação

Este nível é responsável por assegurar que a informação é apresentada ao utilizador de uma forma útil (através do nível de aplicação). O nível de apresentação só trata da sintaxe da informação (a forma como é representada a informação) e não com a sua semântica (significado da informação).

Serviços Fornecidos ao Nível de Aplicação

Os seguintes serviços são fornecidos pelo nível de apresentação:

- Transformação da Sintaxe: trata dos códigos e do conjunto de caracteres a usar (por exemplo o código ASCII), bem como da apresentação da informação (por exemplo a visualização da informação num monitor);
- Selecção da Sintaxe.

Funções do Nível de Apresentação

As funções do nível de apresentação são:

- Negociação e Renegociação da Sintaxe;
- Transformação da Sintaxe;
- Gestão da passagem de serviços dos Níveis Sessão e Aplicação.

2.3.7 O Nível de Aplicação

O nível de apresentação constitui o *interface* entre as aplicações propriamente ditas e o sistema de comunicação. As aplicações trocam informação entre si, utilizando entidades e protocolos do nível de aplicação e serviços do nível de apresentação.

Serviços Fornecidos às Aplicações

Além da transferência da informação, estes serviços podem incluir:

- Identificação dos vários intervenientes da comunicação através do nome, endereço e descrição;
- Determinação da disponibilidade dos intervenientes;
- Verificação e validação dos intervenientes;
- Determinação dos recursos necessários;
- Determinação da qualidade de serviço mínima;
- Sincronização de aplicações;
- Selecção da forma de diálogo;
- Entendimento na responsabilidade na recuperação de erros;
- Acordo na forma de controlo da integridade da informação;
- Identificação de limitações na sintaxe da informação.

Funções do Nível de Aplicação

O nível de aplicação contém todas as funções exigidas pela comunicação entre sistemas abertos, mas que não são fornecidas pelos níveis inferiores. As comunicações entre aplicações são efectuadas através de entidades do nível de aplicação. Estas entidades representam conjuntos de capacidades de comunicação OSI e estão divididas em elementos específicos implementados pelo utilizador e elementos pertencentes aos serviços do nível de aplicação, sendo estes últimos denominados por ASE (Application Service Element).

Um exemplo de um serviço do tipo ASE é o MMS (Manufacturing Message Specification), que é uma norma internacional do nível de aplicação vocacionada para o ambiente industrial.

2.4 A Arquitectura das Comunicações Industriais

Ao nível dos sistemas de controlo a integração implica a necessidade de cooperação e interacção entre os vários subsistemas incluídos no mesmo sistema. Isto significa transferência, armazenamento e processamento de informação em ambientes com características heterogéneas, o que por sua vez obriga à necessidade de dispor de uma infra-estrutura de comunicações adequada. As redes locais industriais, não sendo a solução para este problema, são contudo uma parte integrante e essencial dessa solução.

Os fluxos de informação existentes num ambiente industrial possuem características de tal forma distintas que não é possível dispor de uma única rede capaz de satisfazer todas

as necessidades de comunicação. Desta forma, a alternativa é dispor de um conjunto de redes que no seu conjunto sejam capazes de satisfazer a totalidade dessas necessidades. Num sistema automatizado as actividades relacionadas com o controlo do processo industrial podem ser estruturadas num modelo hierárquico caracterizado por fluxos de informação verticais entre entidades de níveis hierárquicos adjacentes e por fluxos de informação horizontais entre entidades do mesmo nível hierárquico. Como estas actividades estão intimamente associadas à estrutura de comunicações que lhes serve de suporte, surge de forma natural a adopção de um modelo hierárquico para a arquitectura de comunicações (Figura 2.6) [5].

Figura 2.6 - Relação entre os níveis de controlo e a arquitectura de comunicações

Embora os modelos hierárquicos para a estrutura de controlo possam variar em número de níveis, tipicamente entre o 4 e o 6, ao nível da arquitectura de comunicações é usual identificar três níveis distintos: fábrica, célula e campo. Para cada um destes níveis foram desenvolvidas várias soluções, cada uma possuindo diferentes objectivos, protocolos, capacidades e complexidade:

- Fábrica - Cobrem as necessidades dos níveis superiores. As principais actividades encontradas a este nível são o planeamento da produção, de processos e de materiais e as áreas de engenharia financeira e comercial. O fluxo de informações descendente centra-se essencialmente nas ordens de fabrico e nas informações associadas ao seu escalonamento. No sentido ascendente circulam informações relativas ao estado das ordens de fabrico, à qualidade do processo produtivo e a pedidos de aquisição de materiais e/ou recursos. Este nível é caracterizado por um elevado fluxo de informação horizontal entre e dentro dos vários subsistemas existentes sem requisitos temporais críticos.

- Célula - Cobrem as necessidades dos níveis intermédios. Uma célula agrupa um conjunto de equipamentos que cooperam para a execução de uma determinada tarefa. As principais actividades encontradas a este nível são o escalonamento, o sequenciamento e a execução de tarefas. Outras actividades também executadas têm a ver com a compilação da informação relativa à qualidade da produção e ao desempenho dos equipamentos que constituem a célula. A informação que circula do nível célula para os níveis descendentes inclui ordens de execução de operações ou programas de controlo, no caso de equipamentos programáveis. Em sentido ascendente a informação disponibilizada diz respeito à evolução das operações executadas e aos resultados dessas mesmas operações. Este nível é caracterizado por fluxos de informação de volume intermédio e com requisitos temporais exigentes, que em muitos casos podem ser críticos.
- Campo - Cobrem as necessidades dos níveis mais baixos. As principais actividades encontradas a este nível estão relacionadas com o controlo directo do processo industrial, nomeadamente a execução de algoritmos de controlo, por equipamentos que actuam fisicamente sobre os materiais ou produtos a operar. A *interface* com o processo é realizada por intermédio de sensores e actuadores, muitos deles dotados de capacidades de processamento complexas (*smart sensors*). Este nível é caracterizado por fluxos de informação de pequeno volume e com requisitos temporais críticos.

2.5 Redes de Campo

As redes de campo foram inicialmente desenvolvidas com o objectivo de satisfazer os requisitos de comunicação dos níveis mais baixos das arquitecturas de controlo industriais. Entre estes destacam-se, pela sua importância, os seguintes [14], [15]:

- Capacidade de transferir pequenos volumes de informação de forma eficiente;
- suportar tráfego periódico (por exemplo amostragem de dados) e aperiódico (por exemplo eventos) com tempos de resposta majorados. Existem assim requisitos de tempo real associados às comunicações;
- capacidade de operar em ambientes industriais típicos, sujeitos a interferências electromagnéticas, vibrações, corrosão, poeiras, humidade, etc;
- garantir um nível adequado de confiança no funcionamento, nomeadamente no que diz respeito à fiabilidade, disponibilidade e segurança e
- baixo custo de aquisição, instalação, operação e manutenção.

De forma a satisfazer estes requisitos foi adoptada uma *stack* de comunicação organizada de acordo com o modelo OSI, mas compactada em 3 níveis: físico, ligação de dados e aplicação. O nível de aplicação incorpora algumas funcionalidades definidas nos restantes níveis não utilizados neste modelo.

Para cada um dos níveis podem ser definidos múltiplos serviços e protocolos de comunicação com características muito diversas. A escolha destes elementos resulta essencialmente dos objectivos originais definidos pelos fabricantes das redes de campo, que de uma forma sucinta podem ser expressos segundo duas perspectivas [15]:

- A rede de campo é considerada apenas como uma forma de simplificar as ligações físicas entre os vários dispositivos ou
- a rede de campo é considerada a coluna vertebral (*backbone*) de um sistema distribuído e de tempo-real.

A diferença entre estas duas perspectivas foi uma das razões que levaram à proliferação de soluções para as redes de campo. Outras razões estão relacionadas com a ausência de um *standard* internacional único e genérico.

2.5.1 Standardização das Redes de Campo

Já no início dos anos 70 foram instaladas e utilizadas as primeiras redes de campo. No entanto, o trabalho de standardização só teve início em meados dos anos 80. A ideia básica de um *standard* é estabelecer uma especificação de uma forma muito rígida e formal, excluindo a possibilidade de pequenas alterações. Isto dá uma certa noção de confiabilidade e estabilidade da especificação, que por sua vez assegura a confiança dos utilizadores e consequentemente uma boa posição no mercado. Além disso, em muitos países os *standard*s têm uma posição *legally binding*, o que significa que quando um *standard* pode ser aplicado é obrigatório aplicá-lo. Isto implica que um sistema standardizado ganha uma posição competitiva em relação aos rivais não standardizados. Não é então de admirar que fosse iniciada uma corrida para a standardização.

A standardização internacional das redes de campo foi sempre difícil. Teve o seu início em 1985 e, depois de uns anos entusiásticos de desenvolvimento, a procura de um único *standard* foi ficando enredada numa rede de políticas de companhias e de interesses de *marketing* [7].

Na segunda parte dos anos 80, no início dos trabalhos da comissão técnica TC 65C do IEC (International Electrotechnical Commission) o desenvolvimento dos sistemas

fieldbus foi basicamente um projecto europeu, levado a cabo, não só por investigadores com um *background* académico, mas também por muitos proprietários. Os resultados mais promissores foram o francês FIP e o alemão PROFIBUS. Ambos foram standardizados a nível nacional e posteriormente propostos ao IEC para standardização internacional. No entanto, as abordagens dos dois sistemas eram completamente diferentes. O PROFIBUS baseava-se no controlo distribuído e a sua forma original suportava uma comunicação vertical orientada ao objecto, de acordo com o modelo cliente-servidor, no espírito da especificação MAP/MMS. Por outro lado, o FIP foi desenvolvido segundo um esquema de controlo centralizado mas capaz de suportar comunicação em tempo real, de acordo com o novo modelo para comunicação horizontal produtor-consumidor ou *publisher-subscriver*.

Como eram muito diferentes, os dois sistemas satisfaziam os requisitos de áreas de aplicação diferentes. Evidentemente, um *fieldbus* universal tinha de combinar os benefícios dos dois, pelo que um grupo de peritos apresentou uma nova proposta, o WorldFIP, que é uma extensão do FIP ao qual foi acrescentada a funcionalidade do modelo cliente-servidor. Por outro lado, o ISP (Interoperable System Project) tentou demonstrar que o PROFIBUS poderia ser melhorado com a introdução do modelo de comunicação *publisher-subscriber*. No entanto o ISP foi abandonado em 1994 por razões estratégicas [7].

Ao mesmo tempo, o papel de líder nos trabalhos de standardização ao nível do IEC foi sendo tomado, não pelos europeus, mas pelo comité SP50 do ISA (International Society of Automation), que foi muito mais eficiente no fim dos anos 80 e teve uma influência importante na estrutura de camadas do *standard* actual. No entanto, até meados dos anos 90 o comité do IEC não tinha produzido nenhum resultado substancial durante mais de 8 anos. A única excepção foi a definição da camada física, que foi adoptada como um *standard* IEC 61158-2 em 1993.

Em 1995, depois de longos anos de disputas entre investigadores alemães e franceses, com vista a combinar as abordagens FIP e PROFIBUS, várias companhias, basicamente americanas, decidiram não continuar a testemunhar as infindáveis discussões. Com o fim do projecto ISP, iniciaram a definição de uma nova rede de campo optimizada para a indústria de processos: o FF (Fieldbus Foundation). Este trabalho foi feito à parte dos comités IEC, dentro do ISA, e por algum tempo o trabalho no IEC pareceu posto de parte.

A 15 de junho de 1999 o comité de acção do IEC decidiu tomar um novo rumo e um mês depois, a 16 de Junho, os representantes das principais partes interessadas na

standardização *fieldbus* (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, PROFIBUS User Organization e Siemens) assinaram um "Memorando de Entendimento", com o objectivo de pôr um ponto final na disputa dos *standards fieldbus*.

Este processo culminou em 2003 com a adopção de uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 (Digital Data Communications for Measurement and Control - Fieldbus for use in Industrial Control Systems) e o IEC 61784 (Digital Data Communications for Measurement and Control - Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems), sendo ambos constituídos por um conjunto de perfis de comunicação, aos quais acabaram por corresponder as soluções comerciais mais importantes existentes à data da sua publicação (Tabela 2.1) [7].

Tabela 2.1 - Perfis e protocolos de acordo com o IEC 61784 e o IEC 61158

IEC 61784 Perfil	IEC 61158 Protocolos-camadas			Standard CENELEC	Nome comercial
	Física	Ligação de dados	Aplicação		
CPF-1/1	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H1)
CPF-1/2	Ethernet	TCP/UDP/IP	Tipo 5	-	Foundation Fieldbus (HSE)
CPF-1/3	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H2)
CPF-2/1	Tipo 2	Tipo 2	Tipo 2	EN-50170-A3	ControlNet
CPF-2/2	Ethernet	TCP/UDP/IP	Tipo 2	-	Ethernet/IP
CPF-3/1	Tipo 3	Tipo 3	Tipo 3	EN-50254-3	PROFIBUS-DP
CPF-3/2	Tipo 1	Tipo 3	Tipo 3	EN-50170-A2	PROFIBUS-PA
CPF-3/3	Ethernet	TCP/UDP/IP	Tipo 10	-	PROFINET
CPF-4/1	Tipo 3	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-485
CPF-4/1	Tipo 1	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-232
CPF-5/1	Ethernet	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS)
CPF-5/2	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS, subMMS)
CPF-5/3	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS)
CPF-6/1	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS
CPF-6/2	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS TCP/IP
CPF-6/3	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS Subset
CPF-7/1	Tipo 1	Tipo 6	-	-	Swiftnet transport
CPF-7/2	Tipo 1	Tipo 6	Tipo 6	-	Swiftnet full stack

Como se pode verificar pela tabela, sistemas *fieldbus* simples, como o CAN e o AS-*Interface*, não foram incluídos nesta norma. Estes estão incluídos num *standard* específico para este tipo de sistemas, o IEC 62026 (Low-voltage switchgear and controlgear - Controller-Device Interfaces), publicado em Junho de 2007.

À medida que o processo de standardização foi estabilizando, o desenvolvimento focou-se na definição de uma quarta camada, denominada camada de utilizador. O seu objectivo é disponibilizar ao utilizador uma abordagem integrada no desenvolvimento das aplicações, nomeadamente através da definição de blocos funcionais, linguagens de descrição dos dispositivos, interoperabilidade e métricas da qualidade de serviço.

Quanto ao seu posicionamento em relação aos níveis de controlo das aplicações industriais, as redes de campo sofreram uma evolução, passando também a ser utilizadas presentemente como redes de célula. A própria terminologia tem evoluído, através da definição de um conjunto de subcategorias para as redes de campo (Figura 2.7) [5]. Neste sentido, o termo original *fieldbus* tem sido utilizado para designar as redes de campo que estão mais próximas do conceito de rede de célula (ex. PROFIBUS-DP, WorldFIP) e o termo *sensorbus* para designar as redes mais básicas e mais próximas do conceito original de rede de campo (ex. AS-Interface, INTERBUS-S), enquanto o termo *devicebus* é utilizado para designar as que estão num plano de actuação intermédio (ex. DeviceNet, FF-H1). Contudo, e por uma questão de simplificação de linguagem, utiliza-se nesta dissertação apenas os termos rede de campo ou *fieldbus* para representar todas as subcategorias acima definidas.

Figura 2.7 - Categorias das redes de campo

2.6 Ethernet em Tempo Real

Ao mesmo tempo que decorria a standardização *fieldbus*, no mundo administrativo eram implementadas redes baseadas na Ethernet e no TCP/IP. Os custos associados a estas

infra-estruturas têm vindo continuamente a baixar e tornou-se possível ligar quase tudo, em qualquer lado do mundo, com a ajuda da tecnologia da Internet. No entanto, no campo da automação, ainda eram utilizados *fieldbuses* dedicados, a única barreira para aceder a componentes no chão de fábrica via Internet.

Depois de mais de 1 década de experiência com aplicações de *fieldbuses* a indústria começou a desenvolver e a adoptar soluções RTE. Os *standard*s propostos pelo IEC tentam traçar uma linha de orientação e critérios de selecção baseados em indicadores reconhecidos.

A adopção da tecnologia Ethernet na comunicação industrial pressupõe capacidades Internet, como por exemplo *interfaces* com o utilizador remotos, via Web. No entanto, é uma solução inaceitável se a adopção da tecnologia Ethernet causa perda de características necessárias no chão de fábrica, tais como [18]:

- Comunicação determinística;
- acções sincronizadas entre componentes e
- troca de pequenos pacotes de dados eficiente e frequente.

Um requisito implícito e essencial é a capacidade de comunicação Ethernet no nível de escritório ser totalmente absorvida, de modo que o *software* de comunicação envolvido possa ser utilizado. Isto resulta nos seguintes requisitos:

- Suporte de migração da Ethernet do nível do escritório para RTE e
- uso de componentes *standard* (*bridges*, controladores Ethernet e *stack*s de protocolo).

Para se obter a necessária alta qualidade de transmissão de dados, com *jitter* limitado e com perturbações devidas ao tráfego de dados TCP/IP limitadas é necessário desenvolver novos componentes de rede.

Resumindo, a RTE é uma especificação *fieldbus* que utiliza a Ethernet nos dois níveis mais baixos.

2.6.1 Standardização RTE

O *standard* Ethernet não atinge os requisitos do RTE. Existem diferentes propostas na comunidade de investigação para a modificação da tecnologia Ethernet. O mercado também adoptou soluções técnicas adicionais. A seguir são apresentadas as soluções RTE propostas para standardização.

As *interfaces* de comunicação estão estruturadas em diferentes níveis. Na figura 2.8 estão representadas as estruturas possíveis de um protocolo de comunicação RTE [18]. Comum a todas as redes Ethernet é a infraestrutura de cablagem universal.

As aplicações *non real time* utilizam os protocolos Ethernet, tal como definido no ISO 8802-3, e o protocolo TCP/UDP/IP. Utilizam ainda protocolos típicos da Internet, tal como o HTTP ou o FTP.

Figura 2.8 - Estruturas possíveis de uma RTE

Para uma solução RTE existem três diferentes abordagens:

- Na primeira mantêm-se os protocolos TCP/UDP/IP e a modificação que garante o tempo real é feita no nível mais alto. É a solução *on top of* TCP/IP.
- Na segunda não são utilizados os protocolos TCP/UDP/IP e a funcionalidade Ethernet é acedida directamente. É a solução *on top of Ethernet*.
- Na terceira abordagem o mecanismo Ethernet e a própria infraestrutura são modificados de forma a obter uma *performance* em tempo real. É a *Modified Ethernet*.

Na secção seguinte são apresentados os protocolos RTE que existem no mercado.

2.6.2 Protocolos RTE

O IEC 61784-2 (Industrial Communication Networks - Profiles – Part 2: Additional Fieldbus Profiles for Real time Networks based on ISO/IEC 8802-3) é o documento *standard* que especifica pelo menos dez diferentes soluções técnicas para RTE, sendo muitas delas incompatíveis [18] (Tabela 2.2). Alguns dos protocolos propostos apenas

estão definidos, não existindo ainda produtos no mercado. No caso de outros protocolos já existem produtos e aplicações.

Tabela 2.2 - Perfis RTE definidos no IEC 61784

Perfil IEC 61784	**Nomes comerciais**	***Ethertypes***
CPF-2	ControlNet (Ethernet/IP)	(0x0800 IP)
CPF-3	PROFIBUS/PROFINET	0x8892
CPF-4	P-NET	(0x0800 IP)
CPF-10	Vnet/IP	(0x0800 IP)
CPF-11	*TCnet* (Time Critical control network)	0x888B
CPF-12	EtherCAT	0x88A4
CPF-13	EPL (Ethernet PowerLink)	0x88AB
CPF-14	EPA (Ethernet for Plant Automation)	0x88BC
CPF-15	MODBUS – RTPS (Real Time Publisher Subscriber).	(0x0800 IP)
CPF-16	SERCOS (SErial Real time COmmunication System Interface)	0x88CD

Protocolos *on top of* TCP/IP

Algumas soluções RTE utilizam a *stack* do protocolo TCP/UDP/IP sem modificações. Com esta *stack* é possível comunicar de uma forma transparente para além dos limites da rede de campo.

É então possível implementar redes de campo que comuniquem com todos os pontos do mundo, da mesma forma que a tecnologia Internet. No entanto, o manuseamento desta *stack* de protocolo de comunicação requer recursos razoáveis, quer ao nível do processamento, quer ao nível da memória e introduz atrasos não determinísticos na comunicação.

A seguir são apresentadas algumas soluções disponíveis no mercado.

Modbus/TCP

Foi definido pela Schneider Electric e é mantido pela Modbus-IDA. Utiliza o já conhecido Modbus (o *standard* industrial "de facto" desde 1979) sobre uma rede TCP/IP, através da porta 502.

Esta é provavelmente uma das soluções Ethernet mais utilizadas em aplicações industriais e satisfaz os requisitos da classe mais baixa de aplicações, o controlo humano.

É um protocolo muito simples, do tipo *request/reply* (envia uma trama de *request* e recebe uma trama de *reply*). Em adição ao histórico Modbus, este protocolo tem definidas extensões *real time* que utilizam o RTPS. O RTPS prevê dois modelos de comunicação: o

publisher-subscriber, que transfere dados do *publisher* para o *subscriber*, e o CST (Composite State Protocol), que transfere informação de estado de um escritor para um leitor.

Ethernet/IP

Este protocolo foi definido pela Rockwell e é mantido pela ODVA (Open DeviceNet Vendor Association) e pela ControlNet International. Utiliza o CIP, que é comum nas redes Ethernet/IP, ControlNet e DeviceNet.

Este protocolo está incluído no *standard* IEC 61784-1 como CP 2/2 (tipo 2 no IEC 61158) e fornece comunicação *real time* baseada no ISO/IEC 8802-3.

Na Ethernet *full-duplex* não existe a possibilidade de atrasos devidos a colisões. No entanto, as tramas Ethernet podem sofrer atrasos no próprio dispositivo de *switch*, caso a porta de saída esteja ocupada na transmissão de outra trama. Isto pode levar a atrasos não determinísticos, que não são aconselháveis em aplicações em tempo real. Para evitar estes atrasos está definido um mecanismo de prioridades no IEEE 802.3, que permite a atribuição de níveis de prioridade (0 a 7) a tramas Ethernet.

P-NET

O P-NET sobre a especificação IP foi proposto pelo comité nacional dinamarquês e o seu uso destina-se ao ambiente IP. Neste protocolo a comunicação em tempo real P-NET é embebida em pacotes UDP/IP, que tanto podem circular em redes IP como em redes *non* IP.

Uma trama P-NET inclui uma tabela P-Net *route*, que por sua vez é constituída por dois elementos: os endereços da fonte e do destino da própria trama. No caso mais simples de uma rede de campo, estes são os endereços de dois nós da própria rede. Para permitir a comunicação entre dispositivos da rede de campo e dispositivos de uma rede IP os endereços da tabela P-Net *route* terão de ser endereços IP.

De facto, este protocolo apenas especifica a forma como são integradas redes P-NET e redes UDP/IP e não prevê nenhuma medida que assegure um comportamento em tempo real na rede Ethernet.

Vnet/IP

Este protocolo foi desenvolvido pela Yokogama.

Utiliza o TCP/IP para a integração de protocolos Internet, como o HTTP, e de extensões de protocolos *real time*, o RTP (Real Time and reliable datagram Protocol).

Este não é de facto um protocolo RTE, apenas utiliza o protocolo UDP/IP para o transporte do protocolo RTP. Não são tomadas nenhumas medidas especiais que garantam o comportamento determinístico de um protocolo *real time*.

Protocolos *on top of* Ethernet

Estes protocolos RTE não alteram o *hardware* de comunicação Ethernet, mas especificam um tipo de protocolo especial na trama Ethernet, o *Ethertype* (tabela 2.2). Por exemplo, o tipo *standard* para o protocolo IP é *Ethertype*=0X0800. Estes protocolos RTE utilizam, além da *stack* de protocolo IP *standard*, a sua própria *stack* de protocolo identificada com o seu próprio tipo. A tabela 2.2 lista os diferentes valores assignados para as várias soluções.

EPL

Foi definido por Bernecker & Rainer e é mantido pelo grupo de standardização EPL.

Baseia-se num sistema de escalonamento *master-slave* num segmento Ethernet partilhado, o SCNM (Slot Communication Network Management). O *master* é o MN (Managing Node), assegura o acesso em tempo real aos dados cíclicos e apenas permite a comunicação de tramas TCP/IP (*non real time*) em *slots* de tempo reservadas para este tipo de dados. Todos os outros nós são os CNs (Controlled Nodes) e apenas podem enviar dados a pedido do MN.

O ciclo de comunicação de um sistema EPL é composto por quatro períodos: *Start*, *Isochronous*, *Asynchronous* e *Idle* (Figura 2.9) [18]. No período *Start* o MN envia uma trama *multicast* SoC (Start of Cycle), que indica o início do ciclo. No período *Isochronous* o MN envia uma trama *unicast* PReq (Poll Request) para cada um dos CNs e o CN acedido envia uma trama *multicast* PRes (Poll Response). No início do período *Asynchronous* o MN envia uma trama SoA (Start of Asynchronous) e o acesso ao meio é permitido tanto ao MN como a qualquer CN, mas apenas pode ser enviada uma trama ASnd (ASynchronous data). O protocolo tipicamente usado neste período é o UDP/IP. Desta forma a transmissão de dados assíncronos nunca interfere com a transmissão de dados síncronos, o que garante um *timing* preciso na comunicação.

Figura 2.9 - Ciclo de comunicação do EPL

TCnet

É uma proposta da Toshiba. Tal como no EPL, a *interface* TCnet está entre a camada física e a camada de ligação de dados. O acesso MAC (Medium Access Control) típico da Ethernet, o CSMA/CD, é modificado.

O período de transmissão de alta velocidade é composto por um serviço de transmissão de dados cíclico em tempo real (no TCnet utiliza-se a expressão *time critical*) e por um serviço de transmissão assíncrona (no TCnet é denominada como *sporadic*) (Figura 2.10) [18].

Cada período de transmissão de alta velocidade é iniciado com o *broadcast* de uma trama SYN para todos os nós da rede. Depois de receber a trama SYN, o nó 1 inicia a transmissão das suas tramas de dados (DT). Quando termina faz o *broadcast* de uma trama CMP, que indica o fim da sua transmissão. Esta é recebida pelo nó 2, que inicia a transmissão das suas tramas de dados, repetindo-se o processo até ao último nó.

Figura 2.10 - Ciclo de comunicação do TCnet

EPA

O protocolo EPA é uma proposta chinesa.

Este protocolo permite uma comunicação determinística baseada num mecanismo de divisão de tempo dentro da camada MAC. O *macrocycle* (T) é o tempo total para completar um procedimento de transmissão de dados. Esse tempo é dividido em duas fases: a fase para transmissão de mensagens periódicas (Tp) e a fase para transmissão de mensagens aperiódicas (Tn) (Figura 2.11) [18].

A última parte de cada mensagem periódica é um anúncio de mensagem não periódica, que indica se o dispositivo que enviou a mensagem periódica tem ou não uma mensagem não periódica para transmitir. Se tiver, o dispositivo só a poderá enviar na fase Tn.

Figura 2.11 - Ciclo de comunicação do EPA

PROFINET CBA

Foi definido por um conjunto de vários fabricantes, incluindo a Siemens, e é mantido pela PROFIBUS Internacional.

A primeira versão foi baseada no CBA (Component Based Automation) e está incluída no IEC 61784-1 (tipo 10 no IEC 61158).

Para a transmissão de dados sem requisitos de tempo real é utilizada a *stack* TCP/IP e protocolos como o RPC (Remote Procedure Call) e o DCOM (Distributed Component Object Model). Quando é necessária comunicação em tempo real (para ciclos de tempo abaixo dos 100 ms) não é utilizada a *stack* TCP/IP, sendo preferido o protocolo em tempo

real, que é baseado no *Ethertype* 0x8892 e no mecanismo de atribuição de prioridade à trama.

Modified Ethernet

A topologia da cablagem típica da Ethernet é a topologia em estrela: todos os componentes estão ligados a um dispositivo central de *switch*.

Nas aplicações da área da automação, com a introdução do *fieldbus* a topologia em estrela foi substituída por topologias em barramento ou em anel para reduzir os custos na cablagem.

As soluções RTE devem estar preparadas, tanto para as topologias utilizadas no chão de fábrica, como para a topologia da *swicthed Ethernet*. Para isso existem duas soluções: ou a infraestrutura da rede de campo tem um *switch* para cada dispositivo, ou a funcionalidade de *switch* é integrada nos próprios dispositivos da rede de campo.

SERCOS

O SERCOS III é uma extensão RTE do SERCOS, definido pelo *standard* IEC 61491 (Electrical Equipment of Industrial Machines – Serial Data for Real-Time Communication for Controls and Drives), o seu processo de standardização teve início em 2005 e culminou em 2007 com a aprovação do *standard* IEC 61784-2/61158.

No sistema SERCOS existe uma estação *master* e estações *slave*s, cujo número pode variar entre 1 e 254. Todas as estações têm duas portas Ethernet. A topologia da rede pode ser *daisy-chain* ou em anel. Não são permitidos *switches* entre estações e, apenas no caso da topologia *daisy chain*, a porta Ethernet livre do último *slave* pode ser ligada a um *switch*, se for requerida comunicação entre dispositivos via TCP/IP ou UDP/UDP.

No sistema SERCOS III o ciclo de comunicação está dividido em dois períodos, denominados de canais de comunicação: o primeiro é o canal *real time* e o segundo, com menor duração, é o canal *non real time* (Figura 2.12) [18].

O ciclo de comunicação é iniciado pelo *master*, que envia a t*odos os slaves* dois tipos de telegramas *real time*: até 4 MDTs (Master Data Telegrams) e até 4 ATs (Answer Telegrams). Os MDTs contêm informação para sincronização, informação de controlo, dados de serviço do canal e valores de comando. Os ATs são transmitidos pelo *master* como uma trama vazia, mas com campos pré definidos, sendo cada um desses campos destinado a um determinado *slave*. Se um *slave* pretende enviar informação coloca-a no

seu campo e envia o telegrama AT. Quando termina o canal *real time* é iniciado o canal *non real time*, durante o qual podem ser enviados telegramas *non real time*.

Figura 2.12 - Ciclo de comunicação do SERCOS III

ETHERCAT

Este protocolo foi definido pela Beckoff e é mantido pelo grupo de tecnologia Ethercat (ETG). Utiliza as tramas Ethernet e uma topologia em anel especial.

Utiliza um mecanismo de acesso ao meio do tipo *master-slave*, no qual o nó *master* (tipicamente o sistema de controlo) envia tramas *Ethernet standards* ISO/IEC 8802-3 para os nós *slaves*, que por sua vez recebem e enviam dados através dessas tramas.

PROFINET IO

Este protocolo foi definido por vários fabricantes, sendo o mais importante a Siemens, e é mantido pela PROFIBUS Internacional.

Depois da definição PROFINET CBA, o passo seguinte foi a definição de um modelo de aplicação para o PROFINET IO baseado no PROFIBUS DP (tipo 3 do IEC 61158).

Num sistema deste tipo existem três tipos de dispositivos: os controladores IO, os dispositivos IO e o supervisor IO. Os controladores IO controlam os dispositivos IO com comunicação de dados cíclica através de um *buffer*. O supervisor IO gere o funcionamento dos componentes IO e dos controladores IO do sistema.

O ciclo de troca de dados entre os componentes de um sistema PROFINET IO é dividido nas seguintes fases de comunicação: IRT (Isochronous Real Time), RT (Real Time) e NRT (Non Real Time) (Figura 2.13) [18].

Na fase *Isochronous* a comunicação é escalonada no tempo: em cada tempo de offset a trama IRT é enviada de uma porta para outra sem interpretação do endereço por parte do switch. Nas fases seguintes os *switches* comportam-se como *switches standard* Ethernet, passando a comunicação a ser baseada no endereço. Primeiro são transmitidas as tramas RT durante a fase RT e quando esta termina é iniciada a fase NRT, durante a qual são transmitidas as tramas NRT.

Figura 2.13 - Ciclo de comunicação do PROFINET IO

2.7 Conclusão

Neste capítulo foram abordadas as redes de comunicação industriais, tendo sido feita uma análise aos principais protocolos actualmente utilizados.

Pode-se questionar sobre a necessidade do desenvolvimento de tantos protocolos. No entanto, tal facto é justificado, por um lado, pela pressão dos vários grupos económicos e, por outro, pela complexidade e variedade das possíveis áreas de aplicação.

Em relação a este segundo aspecto, é de facto difícil de conceber que uma única norma consiga abranger todas as áreas de aplicação e, nas várias tentativas feitas, provou-se que tal norma se tornava demasiado complexa, tendo um custo de implementação demasiado alto.

Quanto ao primeiro ponto, é evidente que as empresas fabricantes de sistemas e equipamento não tinham, e não têm, interesse em divulgar os protocolos de comunicação, para proteger os investimentos feitos em termos de I&D (Investigação e Desenvolvimento).

No entanto, depois de muitos anos de esforços foi adoptada uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 e o IEC 61784, que englobam as soluções comerciais mais importantes, incluindo soluções RTE.

Compete ao utilizador final e ao mercado decidir quais das soluções propostas preenchem os requisitos das aplicações em automação.

2 Redes de Comunicações Industriais

2.1 Introdução

A evolução da tecnologia nos últimos anos teve uma grande influência na sociedade, levando a caracterizá-la hoje como a sociedade do conhecimento. Com efeito, a globalização é hoje uma realidade, permitindo um rápido acesso à informação onde quer que ela se encontre, originando assim um esforço de actualização constante, já que a informação de que hoje dispomos ficará rapidamente ultrapassada.

O reflexo nas empresas fabris desta maneira de estar da sociedade actual traduz-se em novos desafios, no que respeita à produtividade: o nível de exigência do consumidor aumentou, os ciclos de vida dos produtos diminuíram, as linhas de produção tiveram de ser optimizadas em termos de níveis de *stocks* e flexibilidade, tudo a um baixo custo, para ser possível responder às necessidades do mercado de uma forma rentável. Este desafio nas áreas da inovação e da competitividade obrigou as empresas a concentrar esforços na modernização tecnológica dos seus processos de fabrico, nomeadamente na automatização dos mesmos. Deste esforço integrado resultaram, para além de produtos mais competitivos, o desenvolvimento de soluções tecnológicas avançadas que, à medida que se tornaram cada vez mais comuns e acessíveis, passaram também a ser incorporadas nos próprios processos de fabrico.

Durante as últimas três décadas assistiu-se a uma evolução sem paralelo na área dos sistemas de controlo, nomeadamente ao nível dos respectivos processos de concepção, implementação e operação. Isto deveu-se, em grande parte, aos novos desenvolvimentos, quer em áreas tecnológicas, tais como a microelectrónica e as telecomunicações, quer em áreas associadas à gestão e à integração de sistemas, bem como ao desejo de disponibilizar aos utilizadores finais equipamentos com maiores funcionalidades a custos mais reduzidos.

Este desenvolvimento reflectiu-se também ao nível das comunicações industriais, através da substituição progressiva das tradicionais comunicações ponto-a-ponto pelas

LANs (*Local Area Networks*). Embora inicialmente os motivos desta mudança estivessem relacionados com aspectos económicos, tais como a redução da cablagem e dos custos de manutenção, resultaram posteriormente em enormes vantagens ao nível da descentralização do controlo dos processos, na facilidade de instalação e configuração, na elevada flexibilidade de utilização e na melhoria do desempenho dos sistemas de controlo.

A crescente descentralização ao nível das funções de controlo e a crescente utilização de dispositivos inteligentes baseados em microprocessadores ou microcontroladores, criaram as condições necessárias para o desenvolvimento e proliferação das redes de campo. Estas são um tipo específico de rede local industrial, com o objectivo de interligar controladores, sensores e actuadores, que realizam a *interface* com o processo industrial.

Neste capítulo são analisadas as redes de comunicações industriais, com destaque para as redes de campo, os seus *standards* e as soluções comerciais ao nível das redes com fios. Neste contexto, na secção 1.2 é abordado o sistema de controlo do ambiente industrial, sendo ainda feito um resumo sobre a evolução das tecnologias de controlo. Na secção 1.3 é feita uma descrição do modelo OSI, uma vez que os *standards* de redes de campo são baseados nesse modelo. De seguida, na secção 1.4 é analisada a arquitectura das comunicações industriais, sendo ainda estabelecida uma relação entre esta e os níveis de controlo existentes num ambiente industrial. Na secção 1.5 são abordadas as redes de campo em particular, é feito um breve resumo sobre a história da standardização deste tipo de redes e são ainda apresentados os protocolos incluídos no conjunto de *standards* que especificam este tipo de redes. Por último, na secção 1.6 é abordada a *Ethernet* em tempo real e são apresentadas as soluções RTE (Real Time Ethernet) existentes.

2.2 O Sistema de controlo

O funcionamento de forma correcta e segura de um processo industrial de qualquer natureza é assegurado por intermédio de um sistema de controlo apropriado. Independentemente da dimensão ou da complexidade do processo em causa, o respectivo sistema de controlo pode ser decomposto em três subsistemas com funções bem definidas: o processo controlado, o controlador e o operador humano (Figura 2.1) [5].

Figura 2.1 - Sistema de controlo

O controlador é um equipamento que interage com o seu ambiente através de duas *interfaces* com características distintas:

- a *interface* com o processo controlado é definida como a *interface* de instrumentação;
- a *interface* com o operador humano é definida como a *interface* homem-máquina.
- A *interface* de instrumentação consiste num conjunto de sensores e actuadores que transformam os sinais físicos do processo controlado em sinais com características apropriadas para serem utilizados pelo controlador, e vice-versa. A *interface* homem-máquina consiste num conjunto de dispositivos de entrada e saída, que permitem a interacção com um operador humano. Tipicamente, esta interacção realiza-se ao nível da definição de parâmetros do processo e da supervisão da respectiva evolução.

A função do controlador é controlar a evolução do processo através da execução de um algoritmo de controlo adequado. A partir do processamento da informação obtida, quer directamente do estado do processo através da *interface* de instrumentação, quer fornecida pelo operador humano através da *interface* homem-máquina, o algoritmo de controlo produz um conjunto de comandos que são enviados para o processo através da *interface* de instrumentação. Para realizar estas funções o controlador dispõe de uma estrutura funcional, baseada na utilização de equipamentos adequados ao processo em causa, que suporta a execução do algoritmo de controlo.

Ao nível da estrutura funcional, estes sistemas de controlo podem ser classificados em três tipos de arquitecturas (Figura 2.2) [5].

- Centralizadas - o algoritmo de controlo é executado por um único equipamento;
- Descentralizadas - o algoritmo é executado num único equipamento, mas

algumas tarefas de processamento mais simples (ex. condicionamento e aquisição de sinais) são executadas por outros equipamentos de menor complexidade. Isto implica a existência de uma estrutura de comunicações que permita a interacção e a cooperação entre os vários equipamentos (ex. comunicações série ponto-a-ponto);

- Distribuídas - o algoritmo de controlo encontra-se distribuído por vários equipamentos de complexidade e natureza distintas. Tal como nas arquitecturas descentralizadas, é também necessário dispor de uma estrutura de comunicações adequada, sendo esta, contudo, comparativamente muito mais complexa (ex. rede de campo).

Figura 2.2 - Exemplos de arquitecturas de controlo

2.2.1 Evolução das Tecnologias de Controlo

O advento do computador no início dos anos 60 permitiu que estes passassem também a ser utilizados para implementar funções de controlo. O termo DCC (Direct Digital Control) foi utilizado na época para enfatizar o facto do controlo do processo ser realizado directamente pelo computador. O facto de serem programáveis proporcionou-lhes uma esmagadora vantagem em comparação com as tecnologias de lógica discreta utilizadas até ao momento. Um único equipamento (um computador) concentra em si, quer

as tarefas do controlador, quer as *interfaces* de instrumentação e de homem-máquina. No caso da *interface* de instrumentação, os sensores e actuadores são tipicamente ligados ao controlador através de ligações ponto-a-ponto analógicas (ex. anel de corrente). Em paralelo com este processo, tem também início nos finais do anos 60 o desenvolvimento de máquinas de controlo numérico e de *robots* industriais.

As arquitecturas de controlo desenvolvidas até esta época são essencialmente centralizadas. Contudo, as crescentes exigências da indústria, conjugadas com o desenvolvimento do microprocessador no início dos anos 70, permitiram uma evolução para as primeiras arquitecturas descentralizadas. Esta evolução efectuou-se segundo duas perspectivas [6]:

- uma ao nível das indústrias de processos, com o desenvolvimento dos DCS (Distributed Control Systems) com o objectivo de interligar hierarquicamente os equipamentos de controlo de menor complexidade (por exemplo controladores PID - Proportional Integral Derivative) aos equipamentos de maior complexidade (por exemplo mini-computadores);
- outra ao nível das indústrias de manufactura, onde o PLC, cujo desenvolvimento se deu no início dos anos 70, foi utilizado como elemento central das arquitecturas de controlo.

Em ambas as perspectivas, a interligação entre equipamentos era tipicamente realizada, quer através de ligações ponto-a-ponto analógicas, quer através de ligações digitais, utilizando neste último caso protocolos de comunicação proprietários. Embora esta evolução tenha permitido o desenvolvimento de sistemas de controlo cada vez mais complexos, durante a primeira década da sua utilização, as arquitecturas de controlo continuaram a ser caracterizadas por uma estrutura tipicamente centralizada e só mais tarde se registou uma evolução para soluções do tipo descentralizado.

Entre meados dos anos 80 e inícios dos 90, assistiu-se a uma alteração da estrutura das arquitecturas de controlo através da crescente utilização de redes de comunicação industriais para interligar os equipamentos de controlo. Esta evolução tecnológica foi o ponto de partida das primeiras arquitecturas de controlo descentralizadas baseadas numa estrutura de comunicações digital. Estas arquitecturas, embora mais complexas, permitiram obter um importante conjunto de vantagens, das quais se destacam: menores custos, melhores desempenhos, instalação e manutenção mais simples, modularidade, facilidade

na detecção de erros e avarias, etc. Na sequência desta evolução, surge também nesta época o conceito de CIM (Computer Integrated Manufacturing).

O CIM visa a cooperação entre os diferentes sistemas intervenientes no ambiente de fabrico e engloba todas as actividades com ele relacionadas, desde o projecto e desenvolvimento até ao *marketing* e vendas, passando pelo controlo do fabrico. Para que essa cooperação exista de facto é necessário que haja integração entre os sistemas. A integração significa a possibilidade de os subsistemas da empresa poderem interactuar entre si através de sistemas de comunicações de dados e bases de dados comuns.

Os sistemas de comunicações requerem infraestruturas técnicas (*software* e *hardware*). As comunicações requerem também regras (protocolos), regras essas condicionadas, não apenas por aspectos técnicos, mas também pela funcionalidade exigida.

Uma das representações da filosofia CIM consiste em decompor a empresa em cinco níveis, tal como a figura 2.3 indica.

Empresa	Decisões estratégicas Planeamento a longo prazo
Fábrica	Engenharia de concepção
Área	Controlo supervisor Planeamento de capacidades
Célula	Controladores de células SCADA
Posto de trabalho	Sistemas de controlo local sensores e actuadores

Figura 2.3 - Representação da filosofia CIM

A subdivisão em níveis é baseada, entre outros aspectos, nos tipos de actividades realizadas na empresa e leva, geralmente, ao uso de diferentes tipos de redes de comunicações nos vários níveis.

No interior de cada nível as comunicações horizontais são geralmente asseguradas por uma rede local. As comunicações verticais entre dois níveis adjacentes são resolvidas interligando as redes através de dispositivos de ligação.

A figura 2.4 representa um exemplo de uma arquitectura possível para a hierarquia de comunicações dentro de uma empresa.

Nos níveis superiores da hierarquia as comunicações podem ser caracterizadas como correspondendo à troca de grandes quantidades de informação, que tem de ser processada durante períodos relativamente longos mas com uma frequência relativamente baixa.

Ao contrário, nos níveis inferiores da hierarquia pequenas quantidades de informação precisam de ser processadas de uma forma rápida, com o objectivo de controlar processos industriais em tempo real. Este tipo de transacções tem normalmente uma periodicidade cíclica e uma frequência relativamente elevada.

Pode-se então concluir que não é possível satisfazer todos estes requisitos de transferência de dados com um só tipo de rede.

Figura 2.4 - Representação de uma arquitectura possível para a hierarquia das comunicações de uma empresa

Pode assim propor-se uma classificação hierárquica das comunicações industriais em três grandes grupos, que são: redes de fábrica, redes de célula e redes de campo.

As redes de fábrica abrangem os níveis superiores da hierarquia, enquanto as redes de campo correspondem ao nível mais baixo.

Embora esta evolução abrisse um conjunto enorme de perspectivas ao nível da integração de equipamentos situados em diferentes níveis de controlo, na prática isto acabou por não se verificar, devido ao desenvolvimento de muitas soluções proprietárias. Estas acabaram por limitar as potencialidades das arquitecturas de controlo, nomeadamente

ao nível da integração e da interoperabilidade entre equipamentos. Este problema colocou-se de forma especialmente grave ao nível das redes de campo, com os diferentes fabricantes a tentar impor as suas soluções como o *standard* a utilizar. São alguns exemplos o (PROcess FIeld BUS), o WorldFIP (Factory Instrumentation Protocol), o DeviceNet, o INTERBUS-S, e o AS-Interface (Application Server). Este processo terminou apenas recentemente através da adopção de uma solução de compromisso entre as várias propostas existentes [7]. Ao nível das arquitecturas de controlo registou-se uma tendência para adoptar soluções distribuídas, não só devido à possibilidade de dispor de equipamentos com maiores capacidades de processamento, mas também através do desenvolvimento de arquitecturas de comunicação que suportam elevados níveis de integração entre equipamentos.

Embora a introdução das redes industriais viesse resolver o problema da integração horizontal de equipamentos (situados no mesmo nível de controlo), a integração vertical (entre níveis de controlo) foi sempre um problema em aberto. As soluções apontadas inicialmente passavam pela utilização de equipamentos dedicados (*gateways*) ou pelo desenvolvimento de *software* específico que implementava as tarefas de mapear os serviços de comunicação das diferentes redes. Como estas soluções eram normalmente caras e complexas, surgiu no final dos anos 80 a ideia de desenvolver uma arquitectura de comunicações aberta baseada na estrutura do modelo OSI (*Open Systems Interconnection*). Exemplos destas soluções foram o MAP (Manufacturing Automation Protocol) e o MMS (Manufacturing Message Specification). No entanto, o seu sucesso acabou por ser limitado devido, quer à falta de suporte tecnológico adequado, quer à cumplicidade das soluções propostas.

Em paralelo, nas indústrias de processos a utilização de tecnologias SCADA (Supervisory Control and Data Aquisition) foi vista como uma alternativa mais simples e razoavelmente eficaz na integração vertical. Contudo, devido, quer à ausência de adequação destes sistemas para o problema em causa, quer à proliferação de equipamentos de controlo com características muito diversas, a utilização desta tecnologia acabou por resultar em soluções bastante limitadas.

Nos finais dos anos 90, devido às crescentes exigências de integração com aplicações de nível intermédio e superior, nomeadamente o ERP (Enterprise Resource Planning) e o MES (Manufacturing Execution System), foram desenvolvidas um conjunto de tecnologias de *software* baseadas em plataformas de objectos distribuídos, que disponibilizavam uma

infraestrutura ao nível dos serviços de comunicações, permitindo assim desenvolver de forma eficaz os conceitos de integração vertical e horizontal. São exemplos destas tecnologias o CORBA (Common Object Request Broker Architecture), com uma gama alargada de domínios de aplicação, e o OPC (Object linking and embedding for Process Control), que foi especialmente desenvolvido para satisfazer os requisitos no domínio das aplicações industriais. Este processo apresenta actualmente uma grande dinâmica, com destaque para o desenvolvimento de *standards* com base em arquitecturas de objectos distribuídos especialmente vocacionados para as necessidades dos ambientes industriais: IEC 61499 (Function Blocks for Industrial-Process Measurement and Control Systems) e o IEC 61804 (Function Blocks for Process Control). Como resultado deste trabalho, as arquitecturas de comunicação mais recentes já incorporam muitas destas funcionalidades, das quais se destacam: o CIP (Common Industrial Protocol), o IDA (Interface for Distributed Automation), o HSE *fieldbus* (High Speed Ethernet) e o PROFINET.

Entre os finais dos anos 90 e o início da corrente década verificou-se um fenómeno de migração de tecnologias de uso geral para a área das comunicações industriais. O caso mais paradigmático deu-se com a utilização da rede Ethernet em ambientes industriais (IE - Industrial Ethernet). Este processo teve um profundo impacto na estrutura das comunicações industriais, afectando todos os níveis de controlo. Esta migração deveu-se a vários factores, tais como: a existência de soluções de *hardware* de baixo custo e de elevado desempenho, bem como de protocolos de comunicação abertos e a disponibilização de plataformas de *software* para o desenvolvimento integrado de aplicações distribuídas.

A etapa mais recente desta evolução está centrada na utilização das tecnologias desenvolvidas para Web, tais como UDP/TCP/IP (User Datagram Protocol / Transmission Control Protocol / Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), XML (eXtensible Markup Language), Proxys, Java, ou Jini, para o desenvolvimento de aplicações industriais. A utilização destas tecnologias, para além de estarem largamente difundidas e do seu custo reduzido, vai permitir obter níveis de integração superiores nomeadamente ao nível dos domínios de aplicação externos ao ambiente industrial [11].

Associado ainda a este processo de migração de tecnologias emergentes para as redes industriais, é de salientar a crescente tendência para a utilização de redes de comunicações sem fios (como o IEEE 802.11 ou o IEEE 802.15) em ambientes industriais [9], [10].

2.3 O Modelo de Referência OSI

Convém agora, fazer uma descrição do modelo OSI, uma vez que os protocolos de comunicações industriais a seguir mencionados têm como referência esse modelo.

Num ambiente onde existem equipamentos provenientes de diferentes fabricantes a integração implica a definição de protocolos de comunicação normalizados. A ISO (International Organization for Standardization) definiu o modelo de referência OSI com o objectivo de promover o aparecimento de normas na área das comunicações entre computadores, equivalente ao que na altura se verificava já para as comunicações telefónicas, definidas no âmbito da CCITT (Commité Consultatif International de Telegraphique et Telephonique) [12]. O termo "sistema de arquitectura aberta" indica que se um sistema estiver conforme com o modelo OSI então está aberto a comunicar com qualquer outro que obedeça às mesmas normas. É de salientar que o modelo de referência OSI não especifica por si as normas de comunicação. O seu propósito é apenas fornecer uma arquitectura que sirva de base ao desenvolvimento de normas para sistemas de comunicação.

O modelo de referência OSI define 7 camadas, conforme se indica na figura 2.5.

Figura 2.5 - O modelo de referência OSI

A hierarquia dos níveis vai subindo, desde o nível de maior especificidade até ao mais alto, que é o nível mais genérico.

Os três primeiros níveis fornecem um serviço de rede, ou seja, tratam do transporte da informação. O nível físico trata do meio físico para a transmissão de *bits* de informação, o nível lógico organiza os *bits* de uma forma ordenada em blocos (tramas) e assegura que eles são transmitidos e recebidos de uma forma correcta, enquanto o nível de rede assegura que os pacotes chegam ao seu destino final.

Enquanto o serviço de rede fornecido pelos três níveis inferiores é adequado para transportar informação, algumas aplicações podem ter especificações que as redes não fornecem, como por exemplo uma taxa de erros baixa, um elevado nível de segurança, ou a necessidade de manter uma sequência de pacotes que façam uma mensagem completa. São estes os serviços que o nível de transporte fornece aos níveis superiores.

Os níveis acima do nível de transporte não tratam de mecanismos de transmissão de informação. Esse é o trabalho dos quatro níveis inferiores. No entanto, a informação necessita de ser sincronizada e tratada para que as aplicações entendam. O nível de sessão fornece o serviço de gestão da comunicação entre aplicações.

Outro ponto importante é o formato em que a informação é trocada. Os dois sistemas que estão a comunicar podem ter maneiras diferentes de representar os dados. O nível de apresentação preenche o requisito de identificar e estabelecer uma sintaxe comum, que será utilizada pelos dois sistemas.

O nível mais alto é o nível de aplicação, que constitui a *interface* entre as aplicações propriamente ditas e o sistema de comunicações.

Tendo sido feita uma introdução do modelo, a seguir é feita uma abordagem mais detalhada, especificando, em cada nível: os seus objectivos, os serviços oferecidos ao nível imediatamente superior e as suas funções.

2.3.1 O Nível Físico

O nível físico é responsável por uma transmissão transparente da informação através do meio físico. As funções do nível físico são inteiramente independentes do meio físico em uso, seja este constituído por fio de cobre, cabo coaxial ou fibra óptica. O tipo de meio físico utilizado é completamente escondido ao nível lógico pelo nível físico.

As definições do nível físico podem ser agrupadas da seguinte forma:

- Mecânicas: definem o tipo de conector, as dimensões físicas, as posições dos

pinos, etc;

- Eléctricas: definem as características eléctricas, como por exemplo: níveis eléctricos, impedância, etc;
- Funcionais: definem qual o significado dos níveis eléctricos em determinados pinos do conector;
- Procedimentais: definem as regras (procedimentos) a aplicar às várias funções e também qual a sequência em que determinados eventos podem ocorrer.

Serviços Fornecidos ao Nível Lógico

O nível físico fornece os seguintes serviços ao nível lógico:

- Ligações físicas: o fornecimento de uma transmissão de *bits* perfeitamente transparente entre entidades lógicas. A ligação física estabelece um "circuito de informação" entre dois pontos. A ligação física pode ser estabelecida entre dois pontos ou directamente, ou através de um sistema intermédio;
- Tratamento das unidades de informação: este serviço compreende a transmissão de um *bit* em transmissão série, ou de n *bits* em transmissão paralela. A ligação física pode ser *full-duplex* (a informação é feita nos dois sentidos simultaneamente), *half-duplex* (a informação é feita nos dois sentidos mas alternadamente), ou ainda *simplex* (a informação só é feita num sentido);
- Ligação entre pontos: a ligação entre pontos pode ser ponto-a-ponto ou multiponto;
- Sequenciamento: o nível físico coloca os *bits* no meio físico na mesma ordem que lhe foram fornecidos pelo nível lógico
- Identificação de circuito: o nível físico fornece identificadores que definem univocamente a ligação entre dois sistemas. O nível físico fornece identificadores da ligação entre pontos, que podem ser utilizados pelo nível lógico;
- Recuperação de falhas: o nível lógico é notificado de problemas detectados pelo nível físico;
- Parâmetros fornecidos ao nível lógico: são fornecidos parâmetros ao nível lógico, tais como: taxas de erro, taxas de transmissão, disponibilidade de serviço e atrasos.

Funções do Nível Físico

As seguintes funções são executadas pelo nível físico:

- Estabelecimento e libertação das ligações entre entidades do nível lógico;
- Transmissão de sequências de *bits*: estas podem ser síncronas ou assíncronas;
- Gestão: os protocolos do nível físico tratam de alguns aspectos relacionados com a gestão das actividades deste nível.

2.3.2 O Nível Lógico

O nível lógico isola os níveis superiores das características do meio de transmissão e fornece uma ligação sem erros e de confiança. O nível lógico é estabelecido sobre uma ou mais redes físicas e liga duas identidades em sistemas adjacentes. As ligações lógicas são ponto-a-ponto.

Dentro do nível lógico as sequências de *bits* do nível físico são organizadas em blocos de informação denominados tramas. São funções do nível lógico a sincronização dos *bits* dentro de uma trama, a detecção e correcção de erro (através da retransmissão de pacotes) e ainda o controlo de fluxo (dependendo do estado do sistema de recepção, liga ou desliga a transmissão de pacotes).

Serviços Fornecidos ao Nível de Rede

Os seguintes serviços são fornecidos pelo nível lógico:

- Ligação lógica: o estabelecimento de uma ou mais ligações entre duas entidades;
- Unidades de informação do nível lógico: estas entidades teóricas são mapeadas numa base de uma para uma em unidades do protocolo em uso. Na prática, estas são as tramas transmitidas numa ligação lógica;
- Identificadores lógicos: se requerido pelo nível físico, o nível lógico pode fornecer identificadores dos pontos da ligação lógica;
- Sequenciamento: manutenção da sequência correcta de pacotes;
- Detecção de erros: se for detectado um erro não recuperável pelo nível lógico, então o nível físico será notificado;
- Controlo de Fluxo: o nível de rede pode controlar dinamicamente a taxa a que pode receber os pacotes;
- Parâmetros da qualidade do serviço: estes parâmetros são opcionais e incluem

tempos médios entre erros detectados mas irrecuperáveis, taxa de erro residual, disponibilidade do serviço e débito.

Funções do Nível Lógico

As seguintes funções são efectuadas no nível lógico:

- Estabelecimento e libertação das ligações do nível lógico: como foi referido, esta função faz um mapeamento das unidades de informação em unidades do protocolo, em uso numa forma de uma para uma;
- Separação de ligações lógicas: esta função é feita dividindo uma ligação lógica em várias ligações físicas;
- Delimitação e sincronização: esta é essencialmente uma função de empacotamento, que organiza *bits* (unidades do nível físico) em tramas (unidades lógicas);
- Controlo de sequência: mantém a ordem sequencial dos pacotes transmitidos através da ligação lógica;
- Detecção de erros: esta função detecta erros de transmissão, de formato e de operação, que usualmente aparecem devido a deficiências no meio físico;
- Recuperação de erros: esta função tenta recuperar os erros, geralmente através da retransmissão de pacotes;
- Controlo de fluxo: fornece os serviços de controlo de fluxo já descritos;
- Identificação e troca de parâmetros: efectua a identificação de entidades lógicas e controla a troca de parâmetros;
- Controlo da ligação do circuito de dados: esta função fornece o nível de rede com a informação necessária para controlar e manter o circuito de dados ao nível de rede;
- Gestão: os protocolos do nível físico tratam de alguns aspectos da gestão das actividades deste nível.

2.3.3 O Nível de Rede

A função essencial do nível de rede é fornecer uma transmissão de dados perfeitamente transparente de um nível de transporte de um sistema (por exemplo uma aplicação num terminal) a um nível de transporte de outro sistema (por exemplo a aplicação servidora num computador central).

Em redes complexas, entidades comunicantes no nível de transporte não necessitam de estar próximas, mas ligadas através de um ou mais sistemas intermédios. Nestes casos, o nível de rede fornece funções de encaminhamento. Um exemplo pode ser a ligação de uma rede pública de dados com uma rede privada (por exemplo uma rede bancária) e uma rede local. Os endereços de rede são utilizados para identificar as várias entidades comunicantes no nível de transporte ao nível de rede.

Serviços Fornecidos ao Nível de Transporte

Os seguintes serviços são fornecidos pelo nível de rede:

- Endereços de rede: são fornecidos pelo nível de rede e são usados por entidades do nível de transporte, de forma a identificar univocamente outras entidades do nível de transporte;
- Ligações de rede: fornecem os meios de transferir dados entre entidades do nível de transporte;
- Identificadores de Ligações Rede entre sistemas: o nível de rede fornece às entidades do nível de transporte um identificador de ligação associado univocamente com o endereço de rede;
- Unidades de informação do nível de rede: numa ligação de rede o nível de rede fornece, para transmissão, unidades de informação (pacotes de dados). Estas unidades têm um cabeçalho e um final perfeitamente definidos. A integridade da unidade é verificada no nível de rede;
- Parâmetros de qualidade do serviço: estes parâmetros incluem taxa residual de erros, disponibilidade do serviço, habilidade, débito, atraso no tráfego e atraso no estabelecimento de ligações na rede;
- Notificação de erros: erros irrecuperáveis para o nível de rede são participados ao nível de transporte;
- Sequenciamento: o nível de rede pode fazer a entrega de unidades de informação do nível de rede sequencialmente para uma determinada ligação de rede;
- Controlo de fluxo: a entidade de transporte que está a receber pode fazer com que o Serviço de Rede pare de enviar mais unidades de informação. Este controlo de fluxo pode ou não ser enviado ao outro extremo da ligação;
- Libertação: a entidade de transporte pode pedir a libertação da ligação.

Funções do Nível de Rede

As funções de nível de rede fornecem uma grande variedade de configurações, desde ligações ponto-a-ponto a ligações mais complexas, com uma combinação de várias sub-redes. As seguintes funções são efectuadas:

- Encaminhamento e repetição: as ligações da rede são fornecidas por entidades nos sistemas finais, mas podem ser envolvidas entidades em sistemas intermédios que façam repetição. As funções de encaminhamento determinam um caminho definido entre dois endereços;
- Ligações de rede: esta função fornece ligações entre entidades do nível de transporte, fazendo uso de ligações fornecidas pelo nível lógico;
- Multiplexação de ligações de rede: esta função é usada para multiplexar ligações de rede em ligações lógicas;
- Segmentação e empacotamento: o nível de rede pode segmentar e/ou formar blocos que constituem unidades de informação do nível de rede, para facilitar o transporte;
- Funções de detecção de erros: são utilizadas para verificar se a qualidade dos serviços fornecidos numa rede é mantida. Quando há detecção de erros no nível de rede o nível lógico é notificado. As funções de recuperação de erros dependem da qualidade do Serviço de Rede fornecido;
- Sequenciamento: prevê a entrega sequencial de unidades de informação do Serviço de Rede numa determinada ligação;
- Controlo de fluxo;
- Selecção de serviços: esta função permite que sejam seleccionadas as mesmas funções nos dois sistemas, mesmo quando a ligação se faz entre vários subsistemas.

2.3.4 O Nível de Transporte

O papel do nível de transporte é complementar a rede que está por baixo, de forma a assegurar a qualidade dos serviços requeridos que estão acessíveis ao utilizador.

As funções do nível de transporte estão focalizadas em optimização de custos, controlo de erros, controlo de fluxos, sequenciamento e multiplexagem. O nível de transporte também verifica a existência de duplicados e perdas de informação. Se a ligação de rede for quebrada temporariamente, a ligação de transporte pode ser mantida até que a ligação seja restaurada.

Os protocolos do nível de Transporte são definidos para aceitar uma grande variedade de redes, com várias qualidades de serviços. São cinco as classes de Serviços de Transporte disponíveis:

- A classe 0 é a classe mais simples, sem melhoramentos nos Serviços de Rede;
- A classe 1 adiciona recuperação de erros para redes sujeitas a uma grande frequência de interrupções;
- A classe 2 tem as funções da classe 0 mais multiplexagem;
- A classe 3 tem as funções da classe 1 mais multiplexagem;
- A classe 4 adiciona funções de detecção de erros e de dados fora de sequência.

Serviços Fornecidos ao Nível de Sessão

Os seguintes serviços são fornecidos pelo nível de transporte:

- Estabelecimento de ligações de transporte: as ligações de transporte são estabelecidas entre identidades do nível de sessão e são identificadas pelo endereço de transporte. A qualidade do serviço é negociada entre as entidades do nível de sessão e o serviço de transporte;
- Transferência de dados: fornece a transferência de dados, de acordo com a qualidade de serviço que foi negociada;
- Libertação da ligação de transporte: fornece meios para que qualquer entidade da camada de sessão dos sistemas possa libertar a ligação de transporte.

Funções do Nível de Transporte

As operações no nível de transporte são:

1 Fase de Iniciação

Durante esta fase são efectuadas as seguintes funções:

- Obtenção de uma ligação à rede que corresponda aos requisitos em termos de custos e qualidade de serviço.
- Decisão de multiplexagem ou divisão.
- Estabelecer as unidades de informação do protocolo de transporte óptimas.
- Selecção das funções que devem estar operacionais durante a transferência de dados.
- Mapeamento dos endereços de transporte em endereços de rede.

- Fornecimento de identidade aos endereços de transporte.
- Transferência dos dados.

2 Fase de Transferência

Durante esta fase é executada a transmissão de unidades de informação do protocolo de transporte. Os seguintes serviços podem ser usados ou não, dependendo da classe de serviço seleccionada:

- Sequenciamento;
- Empacotamento;
- Segmentação;
- Multiplexagem ou divisão;
- Controlo de fluxo;
- Detecção e recuperação de erros;
- Transferência dos dados enviados;
- Delimitação das unidades de informação do serviço de transporte;
- Identificação das ligações de transporte.

3 Fase de Libertação

Esta fase inclui as seguintes funções:

- Notificação das razões da libertação.
- Identificação da ligação de transporte libertada.
- Transferência de dados.

2.3.5 O Nível de Sessão

Os requisitos para o nível de sessão reflectem a observação da utilização dos sistemas, pela maior parte dos utilizadores, em picos de actividade que podem ser chamados de sessões. Durante a sessão, o utilizador e o sistema iniciam um diálogo. A primeira função do nível de sessão é estabelecer, manter e gerir este diálogo.

As ligações da camada de Sessão são mapeadas em ligações da camada de transporte numa razão de um para um. Não existe multiplexagem neste nível, mas é possível que várias ligações de sessão usem a mesma ligação de transporte sequencialmente. Simultaneamente, uma ligação de sessão pode usar mais que uma ligação de transporte. Se a ligação de transporte se quebrar, devido a problemas nas camadas inferiores da rede, é possível estabelecer uma nova ligação de transporte sem a intervenção do utilizador ou

mesmo chegar ao seu conhecimento a quebra. Neste caso é o nível de sessão que é o responsável pela ressincronização do diálogo entre os dois sistemas.

Serviços Fornecidos ao Nível de Apresentação

Os seguintes serviços são fornecidos pelo nível de sessão:

- Estabelecimento da ligação entre níveis de sessão: permite que duas entidades do nível de apresentação possam estabelecer uma ligação de sessão entre elas;
- Libertação de ligação: permite que entidades do nível de apresentação possam libertar uma ligação do nível de sessão de uma forma ordeira e sem perda de informação;
- Transferência de dados: permite que uma entidade emissora do nível de apresentação possa transferir uma unidade de informação do nível de sessão a uma entidade receptora do nível de apresentação;
- Serviço de Quarentena: permite à entidade emissora solicitar que algumas unidades de informação, enviadas por uma conexão do nível de sessão, não devam ser enviadas à entidade receptora do nível de apresentação, até ordem contrária enviada pelo emissor;
- Gestão de Interacção: permite que entidades do nível de apresentação comandem explicitamente quem vai controlar certas funções de controlo. São possíveis os seguintes tipos de interacção: dois sentidos simultaneamente, dois sentidos alternadamente, um sentido;
- Sincronização de ligação: este serviço permite que entidades do nível de apresentação definam e identifiquem pontos de sincronização que obriguem uma ligação do nível de sessão a permanecer num determinado estado (*reset*) e que definam qual o ponto de ressincronização;
- Situações excepcionais: faz a notificação ao nível superior de quaisquer situações não englobadas pelos serviços deste nível.

Funções do Nível de Sessão

A maior parte das funções necessárias neste nível estão implícitas aos serviços deste nível:

- Mapeamento das ligações de sessão às ligações de transporte;
- Controlo do fluxo do nível de sessão: o nível de sessão não possui controlo de fluxo. Para evitar aumentar as funções do nível de sessão este controlo é feito no nível de

transporte;

- Recuperação de ligações quebradas: no caso de quebra de ligação do nível de transporte o nível de sessão pode ter as funções necessárias para restabelecer uma nova ligação, de forma a continuar a sessão;
- Libertação da ligação de Sessão: permite que se acabe e liberte a ligação sem perda de informação.

2.3.6 O Nível de Apresentação

Este nível é responsável por assegurar que a informação é apresentada ao utilizador de uma forma útil (através do nível de aplicação). O nível de apresentação só trata da sintaxe da informação (a forma como é representada a informação) e não com a sua semântica (significado da informação).

Serviços Fornecidos ao Nível de Aplicação

Os seguintes serviços são fornecidos pelo nível de apresentação:

- Transformação da Sintaxe: trata dos códigos e do conjunto de caracteres a usar (por exemplo o código ASCII), bem como da apresentação da informação (por exemplo a visualização da informação num monitor);
- Selecção da Sintaxe.

Funções do Nível de Apresentação

As funções do nível de apresentação são:

- Negociação e Renegociação da Sintaxe;
- Transformação da Sintaxe;
- Gestão da passagem de serviços dos Níveis Sessão e Aplicação.

2.3.7 O Nível de Aplicação

O nível de apresentação constitui o *interface* entre as aplicações propriamente ditas e o sistema de comunicação. As aplicações trocam informação entre si, utilizando entidades e protocolos do nível de aplicação e serviços do nível de apresentação.

Serviços Fornecidos às Aplicações

Além da transferência da informação, estes serviços podem incluir:

- Identificação dos vários intervenientes da comunicação através do nome, endereço e descrição;
- Determinação da disponibilidade dos intervenientes;
- Verificação e validação dos intervenientes;
- Determinação dos recursos necessários;
- Determinação da qualidade de serviço mínima;
- Sincronização de aplicações;
- Selecção da forma de diálogo;
- Entendimento na responsabilidade na recuperação de erros;
- Acordo na forma de controlo da integridade da informação;
- Identificação de limitações na sintaxe da informação.

Funções do Nível de Aplicação

O nível de aplicação contém todas as funções exigidas pela comunicação entre sistemas abertos, mas que não são fornecidas pelos níveis inferiores. As comunicações entre aplicações são efectuadas através de entidades do nível de aplicação. Estas entidades representam conjuntos de capacidades de comunicação OSI e estão divididas em elementos específicos implementados pelo utilizador e elementos pertencentes aos serviços do nível de aplicação, sendo estes últimos denominados por ASE (Application Service Element).

Um exemplo de um serviço do tipo ASE é o MMS (Manufacturing Message Specification), que é uma norma internacional do nível de aplicação vocacionada para o ambiente industrial.

2.4 A Arquitectura das Comunicações Industriais

Ao nível dos sistemas de controlo a integração implica a necessidade de cooperação e interacção entre os vários subsistemas incluídos no mesmo sistema. Isto significa transferência, armazenamento e processamento de informação em ambientes com características heterogéneas, o que por sua vez obriga à necessidade de dispor de uma infra-estrutura de comunicações adequada. As redes locais industriais, não sendo a solução para este problema, são contudo uma parte integrante e essencial dessa solução.

Os fluxos de informação existentes num ambiente industrial possuem características de tal forma distintas que não é possível dispor de uma única rede capaz de satisfazer todas

as necessidades de comunicação. Desta forma, a alternativa é dispor de um conjunto de redes que no seu conjunto sejam capazes de satisfazer a totalidade dessas necessidades. Num sistema automatizado as actividades relacionadas com o controlo do processo industrial podem ser estruturadas num modelo hierárquico caracterizado por fluxos de informação verticais entre entidades de níveis hierárquicos adjacentes e por fluxos de informação horizontais entre entidades do mesmo nível hierárquico. Como estas actividades estão intimamente associadas à estrutura de comunicações que lhes serve de suporte, surge de forma natural a adopção de um modelo hierárquico para a arquitectura de comunicações (Figura 2.6) [5].

Figura 2.6 - Relação entre os níveis de controlo e a arquitectura de comunicações

Embora os modelos hierárquicos para a estrutura de controlo possam variar em número de níveis, tipicamente entre o 4 e o 6, ao nível da arquitectura de comunicações é usual identificar três níveis distintos: fábrica, célula e campo. Para cada um destes níveis foram desenvolvidas várias soluções, cada uma possuindo diferentes objectivos, protocolos, capacidades e complexidade:

- Fábrica - Cobrem as necessidades dos níveis superiores. As principais actividades encontradas a este nível são o planeamento da produção, de processos e de materiais e as áreas de engenharia financeira e comercial. O fluxo de informações descendente centra-se essencialmente nas ordens de fabrico e nas informações associadas ao seu escalonamento. No sentido ascendente circulam informações relativas ao estado das ordens de fabrico, à qualidade do processo produtivo e a pedidos de aquisição de materiais e/ou recursos. Este nível é caracterizado por um elevado fluxo de informação horizontal entre e dentro dos vários subsistemas existentes sem requisitos temporais críticos.

- Célula - Cobrem as necessidades dos níveis intermédios. Uma célula agrupa um conjunto de equipamentos que cooperam para a execução de uma determinada tarefa. As principais actividades encontradas a este nível são o escalonamento, o sequenciamento e a execução de tarefas. Outras actividades também executadas têm a ver com a compilação da informação relativa à qualidade da produção e ao desempenho dos equipamentos que constituem a célula. A informação que circula do nível célula para os níveis descendentes inclui ordens de execução de operações ou programas de controlo, no caso de equipamentos programáveis. Em sentido ascendente a informação disponibilizada diz respeito à evolução das operações executadas e aos resultados dessas mesmas operações. Este nível é caracterizado por fluxos de informação de volume intermédio e com requisitos temporais exigentes, que em muitos casos podem ser críticos.
- Campo - Cobrem as necessidades dos níveis mais baixos. As principais actividades encontradas a este nível estão relacionadas com o controlo directo do processo industrial, nomeadamente a execução de algoritmos de controlo, por equipamentos que actuam fisicamente sobre os materiais ou produtos a operar. A *interface* com o processo é realizada por intermédio de sensores e actuadores, muitos deles dotados de capacidades de processamento complexas (*smart sensors*). Este nível é caracterizado por fluxos de informação de pequeno volume e com requisitos temporais críticos.

2.5 Redes de Campo

As redes de campo foram inicialmente desenvolvidas com o objectivo de satisfazer os requisitos de comunicação dos níveis mais baixos das arquitecturas de controlo industriais. Entre estes destacam-se, pela sua importância, os seguintes [14], [15]:

- Capacidade de transferir pequenos volumes de informação de forma eficiente;
- suportar tráfego periódico (por exemplo amostragem de dados) e aperiódico (por exemplo eventos) com tempos de resposta majorados. Existem assim requisitos de tempo real associados às comunicações;
- capacidade de operar em ambientes industriais típicos, sujeitos a interferências electromagnéticas, vibrações, corrosão, poeiras, humidade, etc;
- garantir um nível adequado de confiança no funcionamento, nomeadamente no que diz respeito à fiabilidade, disponibilidade e segurança e
- baixo custo de aquisição, instalação, operação e manutenção.

De forma a satisfazer estes requisitos foi adoptada uma *stack* de comunicação organizada de acordo com o modelo OSI, mas compactada em 3 níveis: físico, ligação de dados e aplicação. O nível de aplicação incorpora algumas funcionalidades definidas nos restantes níveis não utilizados neste modelo.

Para cada um dos níveis podem ser definidos múltiplos serviços e protocolos de comunicação com características muito diversas. A escolha destes elementos resulta essencialmente dos objectivos originais definidos pelos fabricantes das redes de campo, que de uma forma sucinta podem ser expressos segundo duas perspectivas [15]:

- A rede de campo é considerada apenas como uma forma de simplificar as ligações físicas entre os vários dispositivos ou
- a rede de campo é considerada a coluna vertebral (*backbone*) de um sistema distribuído e de tempo-real.

A diferença entre estas duas perspectivas foi uma das razões que levaram à proliferação de soluções para as redes de campo. Outras razões estão relacionadas com a ausência de um *standard* internacional único e genérico.

2.5.1 Standardização das Redes de Campo

Já no início dos anos 70 foram instaladas e utilizadas as primeiras redes de campo. No entanto, o trabalho de standardização só teve início em meados dos anos 80. A ideia básica de um *standard* é estabelecer uma especificação de uma forma muito rígida e formal, excluindo a possibilidade de pequenas alterações. Isto dá uma certa noção de confiabilidade e estabilidade da especificação, que por sua vez assegura a confiança dos utilizadores e consequentemente uma boa posição no mercado. Além disso, em muitos países os *standard*s têm uma posição *legally binding*, o que significa que quando um *standard* pode ser aplicado é obrigatório aplicá-lo. Isto implica que um sistema standardizado ganha uma posição competitiva em relação aos rivais não standardizados. Não é então de admirar que fosse iniciada uma corrida para a standardização.

A standardização internacional das redes de campo foi sempre difícil. Teve o seu início em 1985 e, depois de uns anos entusiásticos de desenvolvimento, a procura de um único *standard* foi ficando enredada numa rede de políticas de companhias e de interesses de *marketing* [7].

Na segunda parte dos anos 80, no início dos trabalhos da comissão técnica TC 65C do IEC (International Electrotechnical Commission) o desenvolvimento dos sistemas

fieldbus foi basicamente um projecto europeu, levado a cabo, não só por investigadores com um *background* académico, mas também por muitos proprietários. Os resultados mais promissores foram o francês FIP e o alemão PROFIBUS. Ambos foram standardizados a nível nacional e posteriormente propostos ao IEC para standardização internacional. No entanto, as abordagens dos dois sistemas eram completamente diferentes. O PROFIBUS baseava-se no controlo distribuído e a sua forma original suportava uma comunicação vertical orientada ao objecto, de acordo com o modelo cliente-servidor, no espírito da especificação MAP/MMS. Por outro lado, o FIP foi desenvolvido segundo um esquema de controlo centralizado mas capaz de suportar comunicação em tempo real, de acordo com o novo modelo para comunicação horizontal produtor-consumidor ou *publisher-subscriver*.

Como eram muito diferentes, os dois sistemas satisfaziam os requisitos de áreas de aplicação diferentes. Evidentemente, um *fieldbus* universal tinha de combinar os benefícios dos dois, pelo que um grupo de peritos apresentou uma nova proposta, o WorldFIP, que é uma extensão do FIP ao qual foi acrescentada a funcionalidade do modelo cliente-servidor. Por outro lado, o ISP (Interoperable System Project) tentou demonstrar que o PROFIBUS poderia ser melhorado com a introdução do modelo de comunicação *publisher-subscriber*. No entanto o ISP foi abandonado em 1994 por razões estratégicas [7].

Ao mesmo tempo, o papel de líder nos trabalhos de standardização ao nível do IEC foi sendo tomado, não pelos europeus, mas pelo comité SP50 do ISA (International Society of Automation), que foi muito mais eficiente no fim dos anos 80 e teve uma influência importante na estrutura de camadas do *standard* actual. No entanto, até meados dos anos 90 o comité do IEC não tinha produzido nenhum resultado substancial durante mais de 8 anos. A única excepção foi a definição da camada física, que foi adoptada como um *standard* IEC 61158-2 em 1993.

Em 1995, depois de longos anos de disputas entre investigadores alemães e franceses, com vista a combinar as abordagens FIP e PROFIBUS, várias companhias, basicamente americanas, decidiram não continuar a testemunhar as infindáveis discussões. Com o fim do projecto ISP, iniciaram a definição de uma nova rede de campo optimizada para a indústria de processos: o FF (Fieldbus Foundation). Este trabalho foi feito à parte dos comités IEC, dentro do ISA, e por algum tempo o trabalho no IEC pareceu posto de parte.

A 15 de junho de 1999 o comité de acção do IEC decidiu tomar um novo rumo e um mês depois, a 16 de Junho, os representantes das principais partes interessadas na

standardização *fieldbus* (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, PROFIBUS User Organization e Siemens) assinaram um "Memorando de Entendimento", com o objectivo de pôr um ponto final na disputa dos *standards fieldbus*.

Este processo culminou em 2003 com a adopção de uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 (Digital Data Communications for Measurement and Control - Fieldbus for use in Industrial Control Systems) e o IEC 61784 (Digital Data Communications for Measurement and Control - Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems), sendo ambos constituídos por um conjunto de perfis de comunicação, aos quais acabaram por corresponder as soluções comerciais mais importantes existentes à data da sua publicação (Tabela 2.1) [7].

Tabela 2.1 - Perfis e protocolos de acordo com o IEC 61784 e o IEC 61158

IEC 61784 Perfil	IEC 61158 Protocolos-camadas			Standard CENELEC	Nome comercial
	Física	Ligação de dados	Aplicação		
CPF-1/1	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H1)
CPF-1/2	Ethernet	TCP/UDP/IP	Tipo 5	-	Foundation Fieldbus (HSE)
CPF-1/3	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H2)
CPF-2/1	Tipo 2	Tipo 2	Tipo 2	EN-50170-A3	ControlNet
CPF-2/2	Ethernet	TCP/UDP/IP	Tipo 2	-	Ethernet/IP
CPF-3/1	Tipo 3	Tipo 3	Tipo 3	EN-50254-3	PROFIBUS-DP
CPF-3/2	Tipo 1	Tipo 3	Tipo 3	EN-50170-A2	PROFIBUS-PA
CPF-3/3	Ethernet	TCP/UDP/IP	Tipo 10	-	PROFINET
CPF-4/1	Tipo 3	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-485
CPF-4/1	Tipo 1	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-232
CPF-5/1	Ethernet	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS)
CPF-5/2	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS, subMMS)
CPF-5/3	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS)
CPF-6/1	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS
CPF-6/2	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS TCP/IP
CPF-6/3	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS Subset
CPF-7/1	Tipo 1	Tipo 6	-	-	Swiftnet transport
CPF-7/2	Tipo 1	Tipo 6	Tipo 6	-	Swiftnet full stack

Como se pode verificar pela tabela, sistemas *fieldbus* simples, como o CAN e o AS-*Interface*, não foram incluídos nesta norma. Estes estão incluídos num *standard* específico para este tipo de sistemas, o IEC 62026 (Low-voltage switchgear and controlgear - Controller-Device Interfaces), publicado em Junho de 2007.

À medida que o processo de standardização foi estabilizando, o desenvolvimento focou-se na definição de uma quarta camada, denominada camada de utilizador. O seu objectivo é disponibilizar ao utilizador uma abordagem integrada no desenvolvimento das aplicações, nomeadamente através da definição de blocos funcionais, linguagens de descrição dos dispositivos, interoperabilidade e métricas da qualidade de serviço.

Quanto ao seu posicionamento em relação aos níveis de controlo das aplicações industriais, as redes de campo sofreram uma evolução, passando também a ser utilizadas presentemente como redes de célula. A própria terminologia tem evoluído, através da definição de um conjunto de subcategorias para as redes de campo (Figura 2.7) [5]. Neste sentido, o termo original *fieldbus* tem sido utilizado para designar as redes de campo que estão mais próximas do conceito de rede de célula (ex. PROFIBUS-DP, WorldFIP) e o termo *sensorbus* para designar as redes mais básicas e mais próximas do conceito original de rede de campo (ex. AS-Interface, INTERBUS-S), enquanto o termo *devicebus* é utilizado para designar as que estão num plano de actuação intermédio (ex. DeviceNet, FF-H1). Contudo, e por uma questão de simplificação de linguagem, utiliza-se nesta dissertação apenas os termos rede de campo ou *fieldbus* para representar todas as subcategorias acima definidas.

Figura 2.7 - Categorias das redes de campo

2.6 Ethernet em Tempo Real

Ao mesmo tempo que decorria a standardização *fieldbus*, no mundo administrativo eram implementadas redes baseadas na Ethernet e no TCP/IP. Os custos associados a estas

infra-estruturas têm vindo continuamente a baixar e tornou-se possível ligar quase tudo, em qualquer lado do mundo, com a ajuda da tecnologia da Internet. No entanto, no campo da automação, ainda eram utilizados *fieldbuses* dedicados, a única barreira para aceder a componentes no chão de fábrica via Internet.

Depois de mais de 1 década de experiência com aplicações de *fieldbuses* a indústria começou a desenvolver e a adoptar soluções RTE. Os *standard*s propostos pelo IEC tentam traçar uma linha de orientação e critérios de selecção baseados em indicadores reconhecidos.

A adopção da tecnologia Ethernet na comunicação industrial pressupõe capacidades Internet, como por exemplo *interfaces* com o utilizador remotos, via Web. No entanto, é uma solução inaceitável se a adopção da tecnologia Ethernet causa perda de características necessárias no chão de fábrica, tais como [18]:

- Comunicação determinística;
- acções sincronizadas entre componentes e
- troca de pequenos pacotes de dados eficiente e frequente.

Um requisito implícito e essencial é a capacidade de comunicação Ethernet no nível de escritório ser totalmente absorvida, de modo que o *software* de comunicação envolvido possa ser utilizado. Isto resulta nos seguintes requisitos:

- Suporte de migração da Ethernet do nível do escritório para RTE e
- uso de componentes *standard* (*bridges*, controladores Ethernet e *stack*s de protocolo).

Para se obter a necessária alta qualidade de transmissão de dados, com *jitter* limitado e com perturbações devidas ao tráfego de dados TCP/IP limitadas é necessário desenvolver novos componentes de rede.

Resumindo, a RTE é uma especificação *fieldbus* que utiliza a Ethernet nos dois níveis mais baixos.

2.6.1 Standardização RTE

O *standard* Ethernet não atinge os requisitos do RTE. Existem diferentes propostas na comunidade de investigação para a modificação da tecnologia Ethernet. O mercado também adoptou soluções técnicas adicionais. A seguir são apresentadas as soluções RTE propostas para standardização.

As *interfaces* de comunicação estão estruturadas em diferentes níveis. Na figura 2.8 estão representadas as estruturas possíveis de um protocolo de comunicação RTE [18]. Comum a todas as redes Ethernet é a infraestrutura de cablagem universal.

As aplicações *non real time* utilizam os protocolos Ethernet, tal como definido no ISO 8802-3, e o protocolo TCP/UDP/IP. Utilizam ainda protocolos típicos da Internet, tal como o HTTP ou o FTP.

Figura 2.8 - Estruturas possíveis de uma RTE

Para uma solução RTE existem três diferentes abordagens:

- Na primeira mantêm-se os protocolos TCP/UDP/IP e a modificação que garante o tempo real é feita no nível mais alto. É a solução *on top of* TCP/IP.
- Na segunda não são utilizados os protocolos TCP/UDP/IP e a funcionalidade Ethernet é acedida directamente. É a solução *on top of Ethernet*.
- Na terceira abordagem o mecanismo Ethernet e a própria infraestrutura são modificados de forma a obter uma *performance* em tempo real. É a *Modified Ethernet*.

Na secção seguinte são apresentados os protocolos RTE que existem no mercado.

2.6.2 Protocolos RTE

O IEC 61784-2 (Industrial Communication Networks - Profiles – Part 2: Additional Fieldbus Profiles for Real time Networks based on ISO/IEC 8802-3) é o documento *standard* que especifica pelo menos dez diferentes soluções técnicas para RTE, sendo muitas delas incompatíveis [18] (Tabela 2.2). Alguns dos protocolos propostos apenas

estão definidos, não existindo ainda produtos no mercado. No caso de outros protocolos já existem produtos e aplicações.

Tabela 2.2 - Perfis RTE definidos no IEC 61784

Perfil IEC 61784	Nomes comerciais	*Ethertypes*
CPF-2	ControlNet (Ethernet/IP)	(0x0800 IP)
CPF-3	PROFIBUS/PROFINET	0x8892
CPF-4	P-NET	(0x0800 IP)
CPF-10	Vnet/IP	(0x0800 IP)
CPF-11	*TCnet* (Time Critical control network)	0x888B
CPF-12	EtherCAT	0x88A4
CPF-13	EPL (Ethernet PowerLink)	0x88AB
CPF-14	EPA (Ethernet for Plant Automation)	0x88BC
CPF-15	MODBUS – RTPS (Real Time Publisher Subscriber).	(0x0800 IP)
CPF-16	SERCOS (SErial Real time COmmunication System Interface)	0x88CD

Protocolos *on top of* TCP/IP

Algumas soluções RTE utilizam a *stack* do protocolo TCP/UDP/IP sem modificações. Com esta *stack* é possível comunicar de uma forma transparente para além dos limites da rede de campo.

É então possível implementar redes de campo que comuniquem com todos os pontos do mundo, da mesma forma que a tecnologia Internet. No entanto, o manuseamento desta *stack* de protocolo de comunicação requer recursos razoáveis, quer ao nível do processamento, quer ao nível da memória e introduz atrasos não determinísticos na comunicação.

A seguir são apresentadas algumas soluções disponíveis no mercado.

Modbus/TCP

Foi definido pela Schneider Electric e é mantido pela Modbus-IDA. Utiliza o já conhecido Modbus (o *standard* industrial “de facto” desde 1979) sobre uma rede TCP/IP, através da porta 502.

Esta é provavelmente uma das soluções Ethernet mais utilizadas em aplicações industriais e satisfaz os requisitos da classe mais baixa de aplicações, o controlo humano.

É um protocolo muito simples, do tipo *request/reply* (envia uma trama de *request* e recebe uma trama de *reply*). Em adição ao histórico Modbus, este protocolo tem definidas extensões *real time* que utilizam o RTPS. O RTPS prevê dois modelos de comunicação: o

publisher-subscriber, que transfere dados do *publisher* para o *subscriber*, e o CST (Composite State Protocol), que transfere informação de estado de um escritor para um leitor.

Ethernet/IP

Este protocolo foi definido pela Rockwell e é mantido pela ODVA (Open DeviceNet Vendor Association) e pela ControlNet International. Utiliza o CIP, que é comum nas redes Ethernet/IP, ControlNet e DeviceNet.

Este protocolo está incluído no *standard* IEC 61784-1 como CP 2/2 (tipo 2 no IEC 61158) e fornece comunicação *real time* baseada no ISO/IEC 8802-3.

Na Ethernet *full-duplex* não existe a possibilidade de atrasos devidos a colisões. No entanto, as tramas Ethernet podem sofrer atrasos no próprio dispositivo de *switch*, caso a porta de saída esteja ocupada na transmissão de outra trama. Isto pode levar a atrasos não determinísticos, que não são aconselháveis em aplicações em tempo real. Para evitar estes atrasos está definido um mecanismo de prioridades no IEEE 802.3, que permite a atribuição de níveis de prioridade (0 a 7) a tramas Ethernet.

P-NET

O P-NET sobre a especificação IP foi proposto pelo comité nacional dinamarquês e o seu uso destina-se ao ambiente IP. Neste protocolo a comunicação em tempo real P-NET é embebida em pacotes UDP/IP, que tanto podem circular em redes IP como em redes *non* IP.

Uma trama P-NET inclui uma tabela P-Net *route*, que por sua vez é constituída por dois elementos: os endereços da fonte e do destino da própria trama. No caso mais simples de uma rede de campo, estes são os endereços de dois nós da própria rede. Para permitir a comunicação entre dispositivos da rede de campo e dispositivos de uma rede IP os endereços da tabela P-Net *route* terão de ser endereços IP.

De facto, este protocolo apenas especifica a forma como são integradas redes P-NET e redes UDP/IP e não prevê nenhuma medida que assegure um comportamento em tempo real na rede Ethernet.

Vnet/IP

Este protocolo foi desenvolvido pela Yokogama.

Utiliza o TCP/IP para a integração de protocolos Internet, como o HTTP, e de extensões de protocolos *real time*, o RTP (Real Time and reliable datagram Protocol).

Este não é de facto um protocolo RTE, apenas utiliza o protocolo UDP/IP para o transporte do protocolo RTP. Não são tomadas nenhumas medidas especiais que garantam o comportamento determinístico de um protocolo *real time*.

Protocolos *on top of* Ethernet

Estes protocolos RTE não alteram o *hardware* de comunicação Ethernet, mas especificam um tipo de protocolo especial na trama Ethernet, o *Ethertype* (tabela 2.2). Por exemplo, o tipo *standard* para o protocolo IP é *Ethertype*=0X0800. Estes protocolos RTE utilizam, além da *stack* de protocolo IP *standard*, a sua própria *stack* de protocolo identificada com o seu próprio tipo. A tabela 2.2 lista os diferentes valores assignados para as várias soluções.

EPL

Foi definido por Bernecker & Rainer e é mantido pelo grupo de standardização EPL.

Baseia-se num sistema de escalonamento *master-slave* num segmento Ethernet partilhado, o SCNM (Slot Communication Network Management). O *master* é o MN (Managing Node), assegura o acesso em tempo real aos dados cíclicos e apenas permite a comunicação de tramas TCP/IP (*non real time*) em *slots* de tempo reservadas para este tipo de dados. Todos os outros nós são os CNs (Controlled Nodes) e apenas podem enviar dados a pedido do MN.

O ciclo de comunicação de um sistema EPL é composto por quatro períodos: *Start*, *Isochronous*, *Asynchronous* e *Idle* (Figura 2.9) [18]. No período *Start* o MN envia uma trama *multicast* SoC (Start of Cycle), que indica o início do ciclo. No período *Isochronous* o MN envia uma trama *unicast* PReq (Poll Request) para cada um dos CNs e o CN acedido envia uma trama *multicast* PRes (Poll Response). No início do período *Asynchronous* o MN envia uma trama SoA (Start of Asynchronous) e o acesso ao meio é permitido tanto ao MN como a qualquer CN, mas apenas pode ser enviada uma trama ASnd (ASynchronous data). O protocolo tipicamente usado neste período é o UDP/IP. Desta forma a transmissão de dados assíncronos nunca interfere com a transmissão de dados síncronos, o que garante um *timing* preciso na comunicação.

Figura 2.9 - Ciclo de comunicação do EPL

TCnet

É uma proposta da Toshiba. Tal como no EPL, a *interface* TCnet está entre a camada física e a camada de ligação de dados. O acesso MAC (Medium Access Control) típico da Ethernet, o CSMA/CD, é modificado.

O período de transmissão de alta velocidade é composto por um serviço de transmissão de dados cíclico em tempo real (no TCnet utiliza-se a expressão *time critical*) e por um serviço de transmissão assíncrona (no TCnet é denominada como *sporadic*) (Figura 2.10) [18].

Cada período de transmissão de alta velocidade é iniciado com o *broadcast* de uma trama SYN para todos os nós da rede. Depois de receber a trama SYN, o nó 1 inicia a transmissão das suas tramas de dados (DT). Quando termina faz o *broadcast* de uma trama CMP, que indica o fim da sua transmissão. Esta é recebida pelo nó 2, que inicia a transmissão das suas tramas de dados, repetindo-se o processo até ao último nó.

Figura 2.10 - Ciclo de comunicação do TCnet

EPA

O protocolo EPA é uma proposta chinesa.

Este protocolo permite uma comunicação determinística baseada num mecanismo de divisão de tempo dentro da camada MAC. O *macrocycle* (T) é o tempo total para completar um procedimento de transmissão de dados. Esse tempo é dividido em duas fases: a fase para transmissão de mensagens periódicas (Tp) e a fase para transmissão de mensagens aperiódicas (Tn) (Figura 2.11) [18].

A última parte de cada mensagem periódica é um anúncio de mensagem não periódica, que indica se o dispositivo que enviou a mensagem periódica tem ou não uma mensagem não periódica para transmitir. Se tiver, o dispositivo só a poderá enviar na fase Tn.

Figura 2.11 - Ciclo de comunicação do EPA

PROFINET CBA

Foi definido por um conjunto de vários fabricantes, incluindo a Siemens, e é mantido pela PROFIBUS Internacional.

A primeira versão foi baseada no CBA (Component Based Automation) e está incluída no IEC 61784-1 (tipo 10 no IEC 61158).

Para a transmissão de dados sem requisitos de tempo real é utilizada a *stack* TCP/IP e protocolos como o RPC (Remote Procedure Call) e o DCOM (Distributed Component Object Model). Quando é necessária comunicação em tempo real (para ciclos de tempo abaixo dos 100 ms) não é utilizada a *stack* TCP/IP, sendo preferido o protocolo em tempo

real, que é baseado no *Ethertype* 0x8892 e no mecanismo de atribuição de prioridade à trama.

Modified Ethernet

A topologia da cablagem típica da Ethernet é a topologia em estrela: todos os componentes estão ligados a um dispositivo central de *switch*.

Nas aplicações da área da automação, com a introdução do *fieldbus* a topologia em estrela foi substituída por topologias em barramento ou em anel para reduzir os custos na cablagem.

As soluções RTE devem estar preparadas, tanto para as topologias utilizadas no chão de fábrica, como para a topologia da *swicthed Ethernet*. Para isso existem duas soluções: ou a infraestrutura da rede de campo tem um *switch* para cada dispositivo, ou a funcionalidade de *switch* é integrada nos próprios dispositivos da rede de campo.

SERCOS

O SERCOS III é uma extensão RTE do SERCOS, definido pelo *standard* IEC 61491 (Electrical Equipment of Industrial Machines – Serial Data for Real-Time Communication for Controls and Drives), o seu processo de standardização teve início em 2005 e culminou em 2007 com a aprovação do *standard* IEC 61784-2/61158.

No sistema SERCOS existe uma estação *master* e estações *slave*s, cujo número pode variar entre 1 e 254. Todas as estações têm duas portas Ethernet. A topologia da rede pode ser *daisy-chain* ou em anel. Não são permitidos *switches* entre estações e, apenas no caso da topologia *daisy chain*, a porta Ethernet livre do último *slave* pode ser ligada a um *switch*, se for requerida comunicação entre dispositivos via TCP/IP ou UDP/UDP.

No sistema SERCOS III o ciclo de comunicação está dividido em dois períodos, denominados de canais de comunicação: o primeiro é o canal *real time* e o segundo, com menor duração, é o canal *non real time* (Figura 2.12) [18].

O ciclo de comunicação é iniciado pelo *master*, que envia a t*odos os slaves* dois tipos de telegramas *real time*: até 4 MDTs (Master Data Telegrams) e até 4 ATs (Answer Telegrams). Os MDTs contêm informação para sincronização, informação de controlo, dados de serviço do canal e valores de comando. Os ATs são transmitidos pelo *master* como uma trama vazia, mas com campos pré definidos, sendo cada um desses campos destinado a um determinado *slave*. Se um *slave* pretende enviar informação coloca-a no

seu campo e envia o telegrama AT. Quando termina o canal *real time* é iniciado o canal *non real time*, durante o qual podem ser enviados telegramas *non real time*.

Figura 2.12 - Ciclo de comunicação do SERCOS III

ETHERCAT

Este protocolo foi definido pela Beckoff e é mantido pelo grupo de tecnologia Ethercat (ETG). Utiliza as tramas Ethernet e uma topologia em anel especial.

Utiliza um mecanismo de acesso ao meio do tipo *master-slave*, no qual o nó *master* (tipicamente o sistema de controlo) envia tramas *Ethernet standards* ISO/IEC 8802-3 para os nós *slaves*, que por sua vez recebem e enviam dados através dessas tramas.

PROFINET IO

Este protocolo foi definido por vários fabricantes, sendo o mais importante a Siemens, e é mantido pela PROFIBUS Internacional.

Depois da definição PROFINET CBA, o passo seguinte foi a definição de um modelo de aplicação para o PROFINET IO baseado no PROFIBUS DP (tipo 3 do IEC 61158).

Num sistema deste tipo existem três tipos de dispositivos: os controladores IO, os dispositivos IO e o supervisor IO. Os controladores IO controlam os dispositivos IO com comunicação de dados cíclica através de um *buffer*. O supervisor IO gere o funcionamento dos componentes IO e dos controladores IO do sistema.

O ciclo de troca de dados entre os componentes de um sistema PROFINET IO é dividido nas seguintes fases de comunicação: IRT (Isochronous Real Time), RT (Real Time) e NRT (Non Real Time) (Figura 2.13) [18].

Na fase *Isochronous* a comunicação é escalonada no tempo: em cada tempo de offset a trama IRT é enviada de uma porta para outra sem interpretação do endereço por parte do switch. Nas fases seguintes os *switches* comportam-se como *switches standard* Ethernet, passando a comunicação a ser baseada no endereço. Primeiro são transmitidas as tramas RT durante a fase RT e quando esta termina é iniciada a fase NRT, durante a qual são transmitidas as tramas NRT.

Figura 2.13 - Ciclo de comunicação do PROFINET IO

2.7 Conclusão

Neste capítulo foram abordadas as redes de comunicação industriais, tendo sido feita uma análise aos principais protocolos actualmente utilizados.

Pode-se questionar sobre a necessidade do desenvolvimento de tantos protocolos. No entanto, tal facto é justificado, por um lado, pela pressão dos vários grupos económicos e, por outro, pela complexidade e variedade das possíveis áreas de aplicação.

Em relação a este segundo aspecto, é de facto difícil de conceber que uma única norma consiga abranger todas as áreas de aplicação e, nas várias tentativas feitas, provou-se que tal norma se tornava demasiado complexa, tendo um custo de implementação demasiado alto.

Quanto ao primeiro ponto, é evidente que as empresas fabricantes de sistemas e equipamento não tinham, e não têm, interesse em divulgar os protocolos de comunicação, para proteger os investimentos feitos em termos de I&D (Investigação e Desenvolvimento).

No entanto, depois de muitos anos de esforços foi adoptada uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 e o IEC 61784, que englobam as soluções comerciais mais importantes, incluindo soluções RTE.

Compete ao utilizador final e ao mercado decidir quais das soluções propostas preenchem os requisitos das aplicações em automação.

2 Redes de Comunicações Industriais

2.1 Introdução

A evolução da tecnologia nos últimos anos teve uma grande influência na sociedade, levando a caracterizá-la hoje como a sociedade do conhecimento. Com efeito, a globalização é hoje uma realidade, permitindo um rápido acesso à informação onde quer que ela se encontre, originando assim um esforço de actualização constante, já que a informação de que hoje dispomos ficará rapidamente ultrapassada.

O reflexo nas empresas fabris desta maneira de estar da sociedade actual traduz-se em novos desafios, no que respeita à produtividade: o nível de exigência do consumidor aumentou, os ciclos de vida dos produtos diminuíram, as linhas de produção tiveram de ser optimizadas em termos de níveis de *stocks* e flexibilidade, tudo a um baixo custo, para ser possível responder às necessidades do mercado de uma forma rentável. Este desafio nas áreas da inovação e da competitividade obrigou as empresas a concentrar esforços na modernização tecnológica dos seus processos de fabrico, nomeadamente na automatização dos mesmos. Deste esforço integrado resultaram, para além de produtos mais competitivos, o desenvolvimento de soluções tecnológicas avançadas que, à medida que se tornaram cada vez mais comuns e acessíveis, passaram também a ser incorporadas nos próprios processos de fabrico.

Durante as últimas três décadas assistiu-se a uma evolução sem paralelo na área dos sistemas de controlo, nomeadamente ao nível dos respectivos processos de concepção, implementação e operação. Isto deveu-se, em grande parte, aos novos desenvolvimentos, quer em áreas tecnológicas, tais como a microelectrónica e as telecomunicações, quer em áreas associadas à gestão e à integração de sistemas, bem como ao desejo de disponibilizar aos utilizadores finais equipamentos com maiores funcionalidades a custos mais reduzidos.

Este desenvolvimento reflectiu-se também ao nível das comunicações industriais, através da substituição progressiva das tradicionais comunicações ponto-a-ponto pelas

LANs (*Local Area Networks*). Embora inicialmente os motivos desta mudança estivessem relacionados com aspectos económicos, tais como a redução da cablagem e dos custos de manutenção, resultaram posteriormente em enormes vantagens ao nível da descentralização do controlo dos processos, na facilidade de instalação e configuração, na elevada flexibilidade de utilização e na melhoria do desempenho dos sistemas de controlo.

A crescente descentralização ao nível das funções de controlo e a crescente utilização de dispositivos inteligentes baseados em microprocessadores ou microcontroladores, criaram as condições necessárias para o desenvolvimento e proliferação das redes de campo. Estas são um tipo específico de rede local industrial, com o objectivo de interligar controladores, sensores e actuadores, que realizam a *interface* com o processo industrial.

Neste capítulo são analisadas as redes de comunicações industriais, com destaque para as redes de campo, os seus *standards* e as soluções comerciais ao nível das redes com fios. Neste contexto, na secção 1.2 é abordado o sistema de controlo do ambiente industrial, sendo ainda feito um resumo sobre a evolução das tecnologias de controlo. Na secção 1.3 é feita uma descrição do modelo OSI, uma vez que os *standards* de redes de campo são baseados nesse modelo. De seguida, na secção 1.4 é analisada a arquitectura das comunicações industriais, sendo ainda estabelecida uma relação entre esta e os níveis de controlo existentes num ambiente industrial. Na secção 1.5 são abordadas as redes de campo em particular, é feito um breve resumo sobre a história da standardização deste tipo de redes e são ainda apresentados os protocolos incluídos no conjunto de *standards* que especificam este tipo de redes. Por último, na secção 1.6 é abordada a *Ethernet* em tempo real e são apresentadas as soluções RTE (Real Time Ethernet) existentes.

2.2 O Sistema de controlo

O funcionamento de forma correcta e segura de um processo industrial de qualquer natureza é assegurado por intermédio de um sistema de controlo apropriado. Independentemente da dimensão ou da complexidade do processo em causa, o respectivo sistema de controlo pode ser decomposto em três subsistemas com funções bem definidas: o processo controlado, o controlador e o operador humano (Figura 2.1) [5].

Figura 2.1 - Sistema de controlo

O controlador é um equipamento que interage com o seu ambiente através de duas *interfaces* com características distintas:

- a *interface* com o processo controlado é definida como a *interface* de instrumentação;
- a *interface* com o operador humano é definida como a *interface* homem-máquina.
- A *interface* de instrumentação consiste num conjunto de sensores e actuadores que transformam os sinais físicos do processo controlado em sinais com características apropriadas para serem utilizados pelo controlador, e vice-versa. A *interface* homem-máquina consiste num conjunto de dispositivos de entrada e saída, que permitem a interacção com um operador humano. Tipicamente, esta interacção realiza-se ao nível da definição de parâmetros do processo e da supervisão da respectiva evolução.

A função do controlador é controlar a evolução do processo através da execução de um algoritmo de controlo adequado. A partir do processamento da informação obtida, quer directamente do estado do processo através da *interface* de instrumentação, quer fornecida pelo operador humano através da *interface* homem-máquina, o algoritmo de controlo produz um conjunto de comandos que são enviados para o processo através da *interface* de instrumentação. Para realizar estas funções o controlador dispõe de uma estrutura funcional, baseada na utilização de equipamentos adequados ao processo em causa, que suporta a execução do algoritmo de controlo.

Ao nível da estrutura funcional, estes sistemas de controlo podem ser classificados em três tipos de arquitecturas (Figura 2.2) [5].

- Centralizadas - o algoritmo de controlo é executado por um único equipamento;
- Descentralizadas - o algoritmo é executado num único equipamento, mas

algumas tarefas de processamento mais simples (ex. condicionamento e aquisição de sinais) são executadas por outros equipamentos de menor complexidade. Isto implica a existência de uma estrutura de comunicações que permita a interacção e a cooperação entre os vários equipamentos (ex. comunicações série ponto-a-ponto);

- Distribuídas - o algoritmo de controlo encontra-se distribuído por vários equipamentos de complexidade e natureza distintas. Tal como nas arquitecturas descentralizadas, é também necessário dispor de uma estrutura de comunicações adequada, sendo esta, contudo, comparativamente muito mais complexa (ex. rede de campo).

Figura 2.2 - Exemplos de arquitecturas de controlo

2.2.1 Evolução das Tecnologias de Controlo

O advento do computador no início dos anos 60 permitiu que estes passassem também a ser utilizados para implementar funções de controlo. O termo DCC (Direct Digital Control) foi utilizado na época para enfatizar o facto do controlo do processo ser realizado directamente pelo computador. O facto de serem programáveis proporcionou-lhes uma esmagadora vantagem em comparação com as tecnologias de lógica discreta utilizadas até ao momento. Um único equipamento (um computador) concentra em si, quer

as tarefas do controlador, quer as *interfaces* de instrumentação e de homem-máquina. No caso da *interface* de instrumentação, os sensores e actuadores são tipicamente ligados ao controlador através de ligações ponto-a-ponto analógicas (ex. anel de corrente). Em paralelo com este processo, tem também início nos finais do anos 60 o desenvolvimento de máquinas de controlo numérico e de *robots* industriais.

As arquitecturas de controlo desenvolvidas até esta época são essencialmente centralizadas. Contudo, as crescentes exigências da indústria, conjugadas com o desenvolvimento do microprocessador no início dos anos 70, permitiram uma evolução para as primeiras arquitecturas descentralizadas. Esta evolução efectuou-se segundo duas perspectivas [6]:

- uma ao nível das indústrias de processos, com o desenvolvimento dos DCS (Distributed Control Systems) com o objectivo de interligar hierarquicamente os equipamentos de controlo de menor complexidade (por exemplo controladores PID - Proportional Integral Derivative) aos equipamentos de maior complexidade (por exemplo mini-computadores);
- outra ao nível das indústrias de manufactura, onde o PLC, cujo desenvolvimento se deu no início dos anos 70, foi utilizado como elemento central das arquitecturas de controlo.

Em ambas as perspectivas, a interligação entre equipamentos era tipicamente realizada, quer através de ligações ponto-a-ponto analógicas, quer através de ligações digitais, utilizando neste último caso protocolos de comunicação proprietários. Embora esta evolução tenha permitido o desenvolvimento de sistemas de controlo cada vez mais complexos, durante a primeira década da sua utilização, as arquitecturas de controlo continuaram a ser caracterizadas por uma estrutura tipicamente centralizada e só mais tarde se registou uma evolução para soluções do tipo descentralizado.

Entre meados dos anos 80 e inícios dos 90, assistiu-se a uma alteração da estrutura das arquitecturas de controlo através da crescente utilização de redes de comunicação industriais para interligar os equipamentos de controlo. Esta evolução tecnológica foi o ponto de partida das primeiras arquitecturas de controlo descentralizadas baseadas numa estrutura de comunicações digital. Estas arquitecturas, embora mais complexas, permitiram obter um importante conjunto de vantagens, das quais se destacam: menores custos, melhores desempenhos, instalação e manutenção mais simples, modularidade, facilidade

na detecção de erros e avarias, etc. Na sequência desta evolução, surge também nesta época o conceito de CIM (Computer Integrated Manufacturing).

O CIM visa a cooperação entre os diferentes sistemas intervenientes no ambiente de fabrico e engloba todas as actividades com ele relacionadas, desde o projecto e desenvolvimento até ao *marketing* e vendas, passando pelo controlo do fabrico. Para que essa cooperação exista de facto é necessário que haja integração entre os sistemas. A integração significa a possibilidade de os subsistemas da empresa poderem interactuar entre si através de sistemas de comunicações de dados e bases de dados comuns.

Os sistemas de comunicações requerem infraestruturas técnicas (*software* e *hardware*). As comunicações requerem também regras (protocolos), regras essas condicionadas, não apenas por aspectos técnicos, mas também pela funcionalidade exigida.

Uma das representações da filosofia CIM consiste em decompor a empresa em cinco níveis, tal como a figura 2.3 indica.

Empresa	Decisões estratégicas Planeamento a longo prazo
Fábrica	Engenharia de concepção
Área	Controlo supervisor Planeamento de capacidades
Célula	Controladores de células SCADA
Posto de trabalho	Sistemas de controlo local sensores e actuadores

Figura 2.3 - Representação da filosofia CIM

A subdivisão em níveis é baseada, entre outros aspectos, nos tipos de actividades realizadas na empresa e leva, geralmente, ao uso de diferentes tipos de redes de comunicações nos vários níveis.

No interior de cada nível as comunicações horizontais são geralmente asseguradas por uma rede local. As comunicações verticais entre dois níveis adjacentes são resolvidas interligando as redes através de dispositivos de ligação.

A figura 2.4 representa um exemplo de uma arquitectura possível para a hierarquia de comunicações dentro de uma empresa.

Nos níveis superiores da hierarquia as comunicações podem ser caracterizadas como correspondendo à troca de grandes quantidades de informação, que tem de ser processada durante períodos relativamente longos mas com uma frequência relativamente baixa.

Ao contrário, nos níveis inferiores da hierarquia pequenas quantidades de informação precisam de ser processadas de uma forma rápida, com o objectivo de controlar processos industriais em tempo real. Este tipo de transacções tem normalmente uma periodicidade cíclica e uma frequência relativamente elevada.

Pode-se então concluir que não é possível satisfazer todos estes requisitos de transferência de dados com um só tipo de rede.

Figura 2.4 - Representação de uma arquitectura possível para a hierarquia das comunicações de uma empresa

Pode assim propor-se uma classificação hierárquica das comunicações industriais em três grandes grupos, que são: redes de fábrica, redes de célula e redes de campo.

As redes de fábrica abrangem os níveis superiores da hierarquia, enquanto as redes de campo correspondem ao nível mais baixo.

Embora esta evolução abrisse um conjunto enorme de perspectivas ao nível da integração de equipamentos situados em diferentes níveis de controlo, na prática isto acabou por não se verificar, devido ao desenvolvimento de muitas soluções proprietárias. Estas acabaram por limitar as potencialidades das arquitecturas de controlo, nomeadamente

ao nível da integração e da interoperabilidade entre equipamentos. Este problema colocou-se de forma especialmente grave ao nível das redes de campo, com os diferentes fabricantes a tentar impor as suas soluções como o *standard* a utilizar. São alguns exemplos o (PROcess FIeld BUS), o WorldFIP (Factory Instrumentation Protocol), o DeviceNet, o INTERBUS-S, e o AS-Interface (Application Server). Este processo terminou apenas recentemente através da adopção de uma solução de compromisso entre as várias propostas existentes [7]. Ao nível das arquitecturas de controlo registou-se uma tendência para adoptar soluções distribuídas, não só devido à possibilidade de dispor de equipamentos com maiores capacidades de processamento, mas também através do desenvolvimento de arquitecturas de comunicação que suportam elevados níveis de integração entre equipamentos.

Embora a introdução das redes industriais viesse resolver o problema da integração horizontal de equipamentos (situados no mesmo nível de controlo), a integração vertical (entre níveis de controlo) foi sempre um problema em aberto. As soluções apontadas inicialmente passavam pela utilização de equipamentos dedicados (*gateways*) ou pelo desenvolvimento de *software* específico que implementava as tarefas de mapear os serviços de comunicação das diferentes redes. Como estas soluções eram normalmente caras e complexas, surgiu no final dos anos 80 a ideia de desenvolver uma arquitectura de comunicações aberta baseada na estrutura do modelo OSI (*Open Systems Interconnection*). Exemplos destas soluções foram o MAP (Manufacturing Automation Protocol) e o MMS (Manufacturing Message Specification). No entanto, o seu sucesso acabou por ser limitado devido, quer à falta de suporte tecnológico adequado, quer à cumplicidade das soluções propostas.

Em paralelo, nas indústrias de processos a utilização de tecnologias SCADA (Supervisory Control and Data Aquisition) foi vista como uma alternativa mais simples e razoavelmente eficaz na integração vertical. Contudo, devido, quer à ausência de adequação destes sistemas para o problema em causa, quer à proliferação de equipamentos de controlo com características muito diversas, a utilização desta tecnologia acabou por resultar em soluções bastante limitadas.

Nos finais dos anos 90, devido às crescentes exigências de integração com aplicações de nível intermédio e superior, nomeadamente o ERP (Enterprise Resource Planning) e o MES (Manufacturing Execution System), foram desenvolvidas um conjunto de tecnologias de *software* baseadas em plataformas de objectos distribuídos, que disponibilizavam uma

infraestrutura ao nível dos serviços de comunicações, permitindo assim desenvolver de forma eficaz os conceitos de integração vertical e horizontal. São exemplos destas tecnologias o CORBA (Common Object Request Broker Architecture), com uma gama alargada de domínios de aplicação, e o OPC (Object linking and embedding for Process Control), que foi especialmente desenvolvido para satisfazer os requisitos no domínio das aplicações industriais. Este processo apresenta actualmente uma grande dinâmica, com destaque para o desenvolvimento de *standards* com base em arquitecturas de objectos distribuídos especialmente vocacionados para as necessidades dos ambientes industriais: IEC 61499 (Function Blocks for Industrial-Process Measurement and Control Systems) e o IEC 61804 (Function Blocks for Process Control). Como resultado deste trabalho, as arquitecturas de comunicação mais recentes já incorporam muitas destas funcionalidades, das quais se destacam: o CIP (Common Industrial Protocol), o IDA (Interface for Distributed Automation), o HSE *fieldbus* (High Speed Ethernet) e o PROFINET.

Entre os finais dos anos 90 e o início da corrente década verificou-se um fenómeno de migração de tecnologias de uso geral para a área das comunicações industriais. O caso mais paradigmático deu-se com a utilização da rede Ethernet em ambientes industriais (IE - Industrial Ethernet). Este processo teve um profundo impacto na estrutura das comunicações industriais, afectando todos os níveis de controlo. Esta migração deveu-se a vários factores, tais como: a existência de soluções de *hardware* de baixo custo e de elevado desempenho, bem como de protocolos de comunicação abertos e a disponibilização de plataformas de *software* para o desenvolvimento integrado de aplicações distribuídas.

A etapa mais recente desta evolução está centrada na utilização das tecnologias desenvolvidas para Web, tais como UDP/TCP/IP (User Datagram Protocol / Transmission Control Protocol / Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), XML (eXtensible Markup Language), Proxys, Java, ou Jini, para o desenvolvimento de aplicações industriais. A utilização destas tecnologias, para além de estarem largamente difundidas e do seu custo reduzido, vai permitir obter níveis de integração superiores nomeadamente ao nível dos domínios de aplicação externos ao ambiente industrial [11].

Associado ainda a este processo de migração de tecnologias emergentes para as redes industriais, é de salientar a crescente tendência para a utilização de redes de comunicações sem fios (como o IEEE 802.11 ou o IEEE 802.15) em ambientes industriais [9], [10].

2.3 O Modelo de Referência OSI

Convém agora, fazer uma descrição do modelo OSI, uma vez que os protocolos de comunicações industriais a seguir mencionados têm como referência esse modelo.

Num ambiente onde existem equipamentos provenientes de diferentes fabricantes a integração implica a definição de protocolos de comunicação normalizados. A ISO (International Organization for Standardization) definiu o modelo de referência OSI com o objectivo de promover o aparecimento de normas na área das comunicações entre computadores, equivalente ao que na altura se verificava já para as comunicações telefónicas, definidas no âmbito da CCITT (Commité Consultatif International de Telegraphique et Telephonique) [12]. O termo "sistema de arquitectura aberta" indica que se um sistema estiver conforme com o modelo OSI então está aberto a comunicar com qualquer outro que obedeça às mesmas normas. É de salientar que o modelo de referência OSI não especifica por si as normas de comunicação. O seu propósito é apenas fornecer uma arquitectura que sirva de base ao desenvolvimento de normas para sistemas de comunicação.

O modelo de referência OSI define 7 camadas, conforme se indica na figura 2.5.

Figura 2.5 - O modelo de referência OSI

A hierarquia dos níveis vai subindo, desde o nível de maior especificidade até ao mais alto, que é o nível mais genérico.

Os três primeiros níveis fornecem um serviço de rede, ou seja, tratam do transporte da informação. O nível físico trata do meio físico para a transmissão de *bits* de informação, o nível lógico organiza os *bits* de uma forma ordenada em blocos (tramas) e assegura que eles são transmitidos e recebidos de uma forma correcta, enquanto o nível de rede assegura que os pacotes chegam ao seu destino final.

Enquanto o serviço de rede fornecido pelos três níveis inferiores é adequado para transportar informação, algumas aplicações podem ter especificações que as redes não fornecem, como por exemplo uma taxa de erros baixa, um elevado nível de segurança, ou a necessidade de manter uma sequência de pacotes que façam uma mensagem completa. São estes os serviços que o nível de transporte fornece aos níveis superiores.

Os níveis acima do nível de transporte não tratam de mecanismos de transmissão de informação. Esse é o trabalho dos quatro níveis inferiores. No entanto, a informação necessita de ser sincronizada e tratada para que as aplicações entendam. O nível de sessão fornece o serviço de gestão da comunicação entre aplicações.

Outro ponto importante é o formato em que a informação é trocada. Os dois sistemas que estão a comunicar podem ter maneiras diferentes de representar os dados. O nível de apresentação preenche o requisito de identificar e estabelecer uma sintaxe comum, que será utilizada pelos dois sistemas.

O nível mais alto é o nível de aplicação, que constitui a *interface* entre as aplicações propriamente ditas e o sistema de comunicações.

Tendo sido feita uma introdução do modelo, a seguir é feita uma abordagem mais detalhada, especificando, em cada nível: os seus objectivos, os serviços oferecidos ao nível imediatamente superior e as suas funções.

2.3.1 O Nível Físico

O nível físico é responsável por uma transmissão transparente da informação através do meio físico. As funções do nível físico são inteiramente independentes do meio físico em uso, seja este constituído por fio de cobre, cabo coaxial ou fibra óptica. O tipo de meio físico utilizado é completamente escondido ao nível lógico pelo nível físico.

As definições do nível físico podem ser agrupadas da seguinte forma:

- Mecânicas: definem o tipo de conector, as dimensões físicas, as posições dos

pinos, etc;

- Eléctricas: definem as características eléctricas, como por exemplo: níveis eléctricos, impedância, etc;
- Funcionais: definem qual o significado dos níveis eléctricos em determinados pinos do conector;
- Procedimentais: definem as regras (procedimentos) a aplicar às várias funções e também qual a sequência em que determinados eventos podem ocorrer.

Serviços Fornecidos ao Nível Lógico

O nível físico fornece os seguintes serviços ao nível lógico:

- Ligações físicas: o fornecimento de uma transmissão de *bits* perfeitamente transparente entre entidades lógicas. A ligação física estabelece um “circuito de informação” entre dois pontos. A ligação física pode ser estabelecida entre dois pontos ou directamente, ou através de um sistema intermédio;
- Tratamento das unidades de informação: este serviço compreende a transmissão de um *bit* em transmissão série, ou de n *bits* em transmissão paralela. A ligação física pode ser *full-duplex* (a informação é feita nos dois sentidos simultaneamente), *half-duplex* (a informação é feita nos dois sentidos mas alternadamente), ou ainda *simplex* (a informação só é feita num sentido);
- Ligação entre pontos: a ligação entre pontos pode ser ponto-a-ponto ou multiponto;
- Sequenciamento: o nível físico coloca os *bits* no meio físico na mesma ordem que lhe foram fornecidos pelo nível lógico
- Identificação de circuito: o nível físico fornece identificadores que definem univocamente a ligação entre dois sistemas. O nível físico fornece identificadores da ligação entre pontos, que podem ser utilizados pelo nível lógico;
- Recuperação de falhas: o nível lógico é notificado de problemas detectados pelo nível físico;
- Parâmetros fornecidos ao nível lógico: são fornecidos parâmetros ao nível lógico, tais como: taxas de erro, taxas de transmissão, disponibilidade de serviço e atrasos.

Funções do Nível Físico

As seguintes funções são executadas pelo nível físico:

- Estabelecimento e libertação das ligações entre entidades do nível lógico;
- Transmissão de sequências de *bits*: estas podem ser síncronas ou assíncronas;
- Gestão: os protocolos do nível físico tratam de alguns aspectos relacionados com a gestão das actividades deste nível.

2.3.2 O Nível Lógico

O nível lógico isola os níveis superiores das características do meio de transmissão e fornece uma ligação sem erros e de confiança. O nível lógico é estabelecido sobre uma ou mais redes físicas e liga duas identidades em sistemas adjacentes. As ligações lógicas são ponto-a-ponto.

Dentro do nível lógico as sequências de *bits* do nível físico são organizadas em blocos de informação denominados tramas. São funções do nível lógico a sincronização dos *bits* dentro de uma trama, a detecção e correcção de erro (através da retransmissão de pacotes) e ainda o controlo de fluxo (dependendo do estado do sistema de recepção, liga ou desliga a transmissão de pacotes).

Serviços Fornecidos ao Nível de Rede

Os seguintes serviços são fornecidos pelo nível lógico:

- Ligação lógica: o estabelecimento de uma ou mais ligações entre duas entidades;
- Unidades de informação do nível lógico: estas entidades teóricas são mapeadas numa base de uma para uma em unidades do protocolo em uso. Na prática, estas são as tramas transmitidas numa ligação lógica;
- Identificadores lógicos: se requerido pelo nível físico, o nível lógico pode fornecer identificadores dos pontos da ligação lógica;
- Sequenciamento: manutenção da sequência correcta de pacotes;
- Detecção de erros: se for detectado um erro não recuperável pelo nível lógico, então o nível físico será notificado;
- Controlo de Fluxo: o nível de rede pode controlar dinamicamente a taxa a que pode receber os pacotes;
- Parâmetros da qualidade do serviço: estes parâmetros são opcionais e incluem

tempos médios entre erros detectados mas irrecuperáveis, taxa de erro residual, disponibilidade do serviço e débito.

Funções do Nível Lógico

As seguintes funções são efectuadas no nível lógico:

- Estabelecimento e libertação das ligações do nível lógico: como foi referido, esta função faz um mapeamento das unidades de informação em unidades do protocolo, em uso numa forma de uma para uma;
- Separação de ligações lógicas: esta função é feita dividindo uma ligação lógica em várias ligações físicas;
- Delimitação e sincronização: esta é essencialmente uma função de empacotamento, que organiza *bits* (unidades do nível físico) em tramas (unidades lógicas);
- Controlo de sequência: mantém a ordem sequencial dos pacotes transmitidos através da ligação lógica;
- Detecção de erros: esta função detecta erros de transmissão, de formato e de operação, que usualmente aparecem devido a deficiências no meio físico;
- Recuperação de erros: esta função tenta recuperar os erros, geralmente através da retransmissão de pacotes;
- Controlo de fluxo: fornece os serviços de controlo de fluxo já descritos;
- Identificação e troca de parâmetros: efectua a identificação de entidades lógicas e controla a troca de parâmetros;
- Controlo da ligação do circuito de dados: esta função fornece o nível de rede com a informação necessária para controlar e manter o circuito de dados ao nível de rede;
- Gestão: os protocolos do nível físico tratam de alguns aspectos da gestão das actividades deste nível.

2.3.3 O Nível de Rede

A função essencial do nível de rede é fornecer uma transmissão de dados perfeitamente transparente de um nível de transporte de um sistema (por exemplo uma aplicação num terminal) a um nível de transporte de outro sistema (por exemplo a aplicação servidora num computador central).

Em redes complexas, entidades comunicantes no nível de transporte não necessitam de estar próximas, mas ligadas através de um ou mais sistemas intermédios. Nestes casos, o nível de rede fornece funções de encaminhamento. Um exemplo pode ser a ligação de uma rede pública de dados com uma rede privada (por exemplo uma rede bancária) e uma rede local. Os endereços de rede são utilizados para identificar as várias entidades comunicantes no nível de transporte ao nível de rede.

Serviços Fornecidos ao Nível de Transporte

Os seguintes serviços são fornecidos pelo nível de rede:

- Endereços de rede: são fornecidos pelo nível de rede e são usados por entidades do nível de transporte, de forma a identificar univocamente outras entidades do nível de transporte;
- Ligações de rede: fornecem os meios de transferir dados entre entidades do nível de transporte;
- Identificadores de Ligações Rede entre sistemas: o nível de rede fornece às entidades do nível de transporte um identificador de ligação associado univocamente com o endereço de rede;
- Unidades de informação do nível de rede: numa ligação de rede o nível de rede fornece, para transmissão, unidades de informação (pacotes de dados). Estas unidades têm um cabeçalho e um final perfeitamente definidos. A integridade da unidade é verificada no nível de rede;
- Parâmetros de qualidade do serviço: estes parâmetros incluem taxa residual de erros, disponibilidade do serviço, habilidade, débito, atraso no tráfego e atraso no estabelecimento de ligações na rede;
- Notificação de erros: erros irrecuperáveis para o nível de rede são participados ao nível de transporte;
- Sequenciamento: o nível de rede pode fazer a entrega de unidades de informação do nível de rede sequencialmente para uma determinada ligação de rede;
- Controlo de fluxo: a entidade de transporte que está a receber pode fazer com que o Serviço de Rede pare de enviar mais unidades de informação. Este controlo de fluxo pode ou não ser enviado ao outro extremo da ligação;
- Libertação: a entidade de transporte pode pedir a libertação da ligação.

Funções do Nível de Rede

As funções de nível de rede fornecem uma grande variedade de configurações, desde ligações ponto-a-ponto a ligações mais complexas, com uma combinação de várias sub-redes. As seguintes funções são efectuadas:

- Encaminhamento e repetição: as ligações da rede são fornecidas por entidades nos sistemas finais, mas podem ser envolvidas entidades em sistemas intermédios que façam repetição. As funções de encaminhamento determinam um caminho definido entre dois endereços;
- Ligações de rede: esta função fornece ligações entre entidades do nível de transporte, fazendo uso de ligações fornecidas pelo nível lógico;
- Multiplexação de ligações de rede: esta função é usada para multiplexar ligações de rede em ligações lógicas;
- Segmentação e empacotamento: o nível de rede pode segmentar e/ou formar blocos que constituem unidades de informação do nível de rede, para facilitar o transporte;
- Funções de detecção de erros: são utilizadas para verificar se a qualidade dos serviços fornecidos numa rede é mantida. Quando há detecção de erros no nível de rede o nível lógico é notificado. As funções de recuperação de erros dependem da qualidade do Serviço de Rede fornecido;
- Sequenciamento: prevê a entrega sequencial de unidades de informação do Serviço de Rede numa determinada ligação;
- Controlo de fluxo;
- Selecção de serviços: esta função permite que sejam seleccionadas as mesmas funções nos dois sistemas, mesmo quando a ligação se faz entre vários subsistemas.

2.3.4 O Nível de Transporte

O papel do nível de transporte é complementar a rede que está por baixo, de forma a assegurar a qualidade dos serviços requeridos que estão acessíveis ao utilizador.

As funções do nível de transporte estão focalizadas em optimização de custos, controlo de erros, controlo de fluxos, sequenciamento e multiplexagem. O nível de transporte também verifica a existência de duplicados e perdas de informação. Se a ligação de rede for quebrada temporariamente, a ligação de transporte pode ser mantida até que a ligação seja restaurada.

Os protocolos do nível de Transporte são definidos para aceitar uma grande variedade de redes, com várias qualidades de serviços. São cinco as classes de Serviços de Transporte disponíveis:

- A classe 0 é a classe mais simples, sem melhoramentos nos Serviços de Rede;
- A classe 1 adiciona recuperação de erros para redes sujeitas a uma grande frequência de interrupções;
- A classe 2 tem as funções da classe 0 mais multiplexagem;
- A classe 3 tem as funções da classe 1 mais multiplexagem;
- A classe 4 adiciona funções de detecção de erros e de dados fora de sequência.

Serviços Fornecidos ao Nível de Sessão

Os seguintes serviços são fornecidos pelo nível de transporte:

- Estabelecimento de ligações de transporte: as ligações de transporte são estabelecidas entre identidades do nível de sessão e são identificadas pelo endereço de transporte. A qualidade do serviço é negociada entre as entidades do nível de sessão e o serviço de transporte;
- Transferência de dados: fornece a transferência de dados, de acordo com a qualidade de serviço que foi negociada;
- Libertação da ligação de transporte: fornece meios para que qualquer entidade da camada de sessão dos sistemas possa libertar a ligação de transporte.

Funções do Nível de Transporte

As operações no nível de transporte são:

1 Fase de Iniciação

Durante esta fase são efectuadas as seguintes funções:

- Obtenção de uma ligação à rede que corresponda aos requisitos em termos de custos e qualidade de serviço.
- Decisão de multiplexagem ou divisão.
- Estabelecer as unidades de informação do protocolo de transporte óptimas.
- Selecção das funções que devem estar operacionais durante a transferência de dados.
- Mapeamento dos endereços de transporte em endereços de rede.

- Fornecimento de identidade aos endereços de transporte.
- Transferência dos dados.

2 Fase de Transferência

Durante esta fase é executada a transmissão de unidades de informação do protocolo de transporte. Os seguintes serviços podem ser usados ou não, dependendo da classe de serviço seleccionada:

- Sequenciamento;
- Empacotamento;
- Segmentação;
- Multiplexagem ou divisão;
- Controlo de fluxo;
- Detecção e recuperação de erros;
- Transferência dos dados enviados;
- Delimitação das unidades de informação do serviço de transporte;
- Identificação das ligações de transporte.

3 Fase de Libertação

Esta fase inclui as seguintes funções:

- Notificação das razões da libertação.
- Identificação da ligação de transporte libertada.
- Transferência de dados.

2.3.5 O Nível de Sessão

Os requisitos para o nível de sessão reflectem a observação da utilização dos sistemas, pela maior parte dos utilizadores, em picos de actividade que podem ser chamados de sessões. Durante a sessão, o utilizador e o sistema iniciam um diálogo. A primeira função do nível de sessão é estabelecer, manter e gerir este diálogo.

As ligações da camada de Sessão são mapeadas em ligações da camada de transporte numa razão de um para um. Não existe multiplexagem neste nível, mas é possível que várias ligações de sessão usem a mesma ligação de transporte sequencialmente. Simultaneamente, uma ligação de sessão pode usar mais que uma ligação de transporte. Se a ligação de transporte se quebrar, devido a problemas nas camadas inferiores da rede, é possível estabelecer uma nova ligação de transporte sem a intervenção do utilizador ou

mesmo chegar ao seu conhecimento a quebra. Neste caso é o nível de sessão que é o responsável pela ressincronização do diálogo entre os dois sistemas.

Serviços Fornecidos ao Nível de Apresentação

Os seguintes serviços são fornecidos pelo nível de sessão:

- Estabelecimento da ligação entre níveis de sessão: permite que duas entidades do nível de apresentação possam estabelecer uma ligação de sessão entre elas;
- Libertação de ligação: permite que entidades do nível de apresentação possam libertar uma ligação do nível de sessão de uma forma ordeira e sem perda de informação;
- Transferência de dados: permite que uma entidade emissora do nível de apresentação possa transferir uma unidade de informação do nível de sessão a uma entidade receptora do nível de apresentação;
- Serviço de Quarentena: permite à entidade emissora solicitar que algumas unidades de informação, enviadas por uma conexão do nível de sessão, não devam ser enviadas à entidade receptora do nível de apresentação, até ordem contrária enviada pelo emissor;
- Gestão de Interacção: permite que entidades do nível de apresentação comandem explicitamente quem vai controlar certas funções de controlo. São possíveis os seguintes tipos de interacção: dois sentidos simultaneamente, dois sentidos alternadamente, um sentido;
- Sincronização de ligação: este serviço permite que entidades do nível de apresentação definam e identifiquem pontos de sincronização que obriguem uma ligação do nível de sessão a permanecer num determinado estado (*reset*) e que definam qual o ponto de ressincronização;
- Situações excepcionais: faz a notificação ao nível superior de quaisquer situações não englobadas pelos serviços deste nível.

Funções do Nível de Sessão

A maior parte das funções necessárias neste nível estão implícitas aos serviços deste nível:

- Mapeamento das ligações de sessão às ligações de transporte;
- Controlo do fluxo do nível de sessão: o nível de sessão não possui controlo de fluxo. Para evitar aumentar as funções do nível de sessão este controlo é feito no nível de

transporte;

- Recuperação de ligações quebradas: no caso de quebra de ligação do nível de transporte o nível de sessão pode ter as funções necessárias para restabelecer uma nova ligação, de forma a continuar a sessão;
- Libertação da ligação de Sessão: permite que se acabe e liberte a ligação sem perda de informação.

2.3.6 O Nível de Apresentação

Este nível é responsável por assegurar que a informação é apresentada ao utilizador de uma forma útil (através do nível de aplicação). O nível de apresentação só trata da sintaxe da informação (a forma como é representada a informação) e não com a sua semântica (significado da informação).

Serviços Fornecidos ao Nível de Aplicação

Os seguintes serviços são fornecidos pelo nível de apresentação:

- Transformação da Sintaxe: trata dos códigos e do conjunto de caracteres a usar (por exemplo o código ASCII), bem como da apresentação da informação (por exemplo a visualização da informação num monitor);
- Selecção da Sintaxe.

Funções do Nível de Apresentação

As funções do nível de apresentação são:

- Negociação e Renegociação da Sintaxe;
- Transformação da Sintaxe;
- Gestão da passagem de serviços dos Níveis Sessão e Aplicação.

2.3.7 O Nível de Aplicação

O nível de apresentação constitui o *interface* entre as aplicações propriamente ditas e o sistema de comunicação. As aplicações trocam informação entre si, utilizando entidades e protocolos do nível de aplicação e serviços do nível de apresentação.

Serviços Fornecidos às Aplicações

Além da transferência da informação, estes serviços podem incluir:

- Identificação dos vários intervenientes da comunicação através do nome, endereço e descrição;
- Determinação da disponibilidade dos intervenientes;
- Verificação e validação dos intervenientes;
- Determinação dos recursos necessários;
- Determinação da qualidade de serviço mínima;
- Sincronização de aplicações;
- Selecção da forma de diálogo;
- Entendimento na responsabilidade na recuperação de erros;
- Acordo na forma de controlo da integridade da informação;
- Identificação de limitações na sintaxe da informação.

Funções do Nível de Aplicação

O nível de aplicação contém todas as funções exigidas pela comunicação entre sistemas abertos, mas que não são fornecidas pelos níveis inferiores. As comunicações entre aplicações são efectuadas através de entidades do nível de aplicação. Estas entidades representam conjuntos de capacidades de comunicação OSI e estão divididas em elementos específicos implementados pelo utilizador e elementos pertencentes aos serviços do nível de aplicação, sendo estes últimos denominados por ASE (Application Service Element).

Um exemplo de um serviço do tipo ASE é o MMS (Manufacturing Message Specification), que é uma norma internacional do nível de aplicação vocacionada para o ambiente industrial.

2.4 A Arquitectura das Comunicações Industriais

Ao nível dos sistemas de controlo a integração implica a necessidade de cooperação e interacção entre os vários subsistemas incluídos no mesmo sistema. Isto significa transferência, armazenamento e processamento de informação em ambientes com características heterogéneas, o que por sua vez obriga à necessidade de dispor de uma infra-estrutura de comunicações adequada. As redes locais industriais, não sendo a solução para este problema, são contudo uma parte integrante e essencial dessa solução.

Os fluxos de informação existentes num ambiente industrial possuem características de tal forma distintas que não é possível dispor de uma única rede capaz de satisfazer todas

as necessidades de comunicação. Desta forma, a alternativa é dispor de um conjunto de redes que no seu conjunto sejam capazes de satisfazer a totalidade dessas necessidades. Num sistema automatizado as actividades relacionadas com o controlo do processo industrial podem ser estruturadas num modelo hierárquico caracterizado por fluxos de informação verticais entre entidades de níveis hierárquicos adjacentes e por fluxos de informação horizontais entre entidades do mesmo nível hierárquico. Como estas actividades estão intimamente associadas à estrutura de comunicações que lhes serve de suporte, surge de forma natural a adopção de um modelo hierárquico para a arquitectura de comunicações (Figura 2.6) [5].

Figura 2.6 - Relação entre os níveis de controlo e a arquitectura de comunicações

Embora os modelos hierárquicos para a estrutura de controlo possam variar em número de níveis, tipicamente entre o 4 e o 6, ao nível da arquitectura de comunicações é usual identificar três níveis distintos: fábrica, célula e campo. Para cada um destes níveis foram desenvolvidas várias soluções, cada uma possuindo diferentes objectivos, protocolos, capacidades e complexidade:

- Fábrica - Cobrem as necessidades dos níveis superiores. As principais actividades encontradas a este nível são o planeamento da produção, de processos e de materiais e as áreas de engenharia financeira e comercial. O fluxo de informações descendente centra-se essencialmente nas ordens de fabrico e nas informações associadas ao seu escalonamento. No sentido ascendente circulam informações relativas ao estado das ordens de fabrico, à qualidade do processo produtivo e a pedidos de aquisição de materiais e/ou recursos. Este nível é caracterizado por um elevado fluxo de informação horizontal entre e dentro dos vários subsistemas existentes sem requisitos temporais críticos.

- Célula - Cobrem as necessidades dos níveis intermédios. Uma célula agrupa um conjunto de equipamentos que cooperam para a execução de uma determinada tarefa. As principais actividades encontradas a este nível são o escalonamento, o sequenciamento e a execução de tarefas. Outras actividades também executadas têm a ver com a compilação da informação relativa à qualidade da produção e ao desempenho dos equipamentos que constituem a célula. A informação que circula do nível célula para os níveis descendentes inclui ordens de execução de operações ou programas de controlo, no caso de equipamentos programáveis. Em sentido ascendente a informação disponibilizada diz respeito à evolução das operações executadas e aos resultados dessas mesmas operações. Este nível é caracterizado por fluxos de informação de volume intermédio e com requisitos temporais exigentes, que em muitos casos podem ser críticos.
- Campo - Cobrem as necessidades dos níveis mais baixos. As principais actividades encontradas a este nível estão relacionadas com o controlo directo do processo industrial, nomeadamente a execução de algoritmos de controlo, por equipamentos que actuam fisicamente sobre os materiais ou produtos a operar. A *interface* com o processo é realizada por intermédio de sensores e actuadores, muitos deles dotados de capacidades de processamento complexas (*smart sensors*). Este nível é caracterizado por fluxos de informação de pequeno volume e com requisitos temporais críticos.

2.5 Redes de Campo

As redes de campo foram inicialmente desenvolvidas com o objectivo de satisfazer os requisitos de comunicação dos níveis mais baixos das arquitecturas de controlo industriais. Entre estes destacam-se, pela sua importância, os seguintes [14], [15]:

- Capacidade de transferir pequenos volumes de informação de forma eficiente;
- suportar tráfego periódico (por exemplo amostragem de dados) e aperiódico (por exemplo eventos) com tempos de resposta majorados. Existem assim requisitos de tempo real associados às comunicações;
- capacidade de operar em ambientes industriais típicos, sujeitos a interferências electromagnéticas, vibrações, corrosão, poeiras, humidade, etc;
- garantir um nível adequado de confiança no funcionamento, nomeadamente no que diz respeito à fiabilidade, disponibilidade e segurança e
- baixo custo de aquisição, instalação, operação e manutenção.

De forma a satisfazer estes requisitos foi adoptada uma *stack* de comunicação organizada de acordo com o modelo OSI, mas compactada em 3 níveis: físico, ligação de dados e aplicação. O nível de aplicação incorpora algumas funcionalidades definidas nos restantes níveis não utilizados neste modelo.

Para cada um dos níveis podem ser definidos múltiplos serviços e protocolos de comunicação com características muito diversas. A escolha destes elementos resulta essencialmente dos objectivos originais definidos pelos fabricantes das redes de campo, que de uma forma sucinta podem ser expressos segundo duas perspectivas [15]:

- A rede de campo é considerada apenas como uma forma de simplificar as ligações físicas entre os vários dispositivos ou
- a rede de campo é considerada a coluna vertebral (*backbone*) de um sistema distribuído e de tempo-real.

A diferença entre estas duas perspectivas foi uma das razões que levaram à proliferação de soluções para as redes de campo. Outras razões estão relacionadas com a ausência de um *standard* internacional único e genérico.

2.5.1 Standardização das Redes de Campo

Já no início dos anos 70 foram instaladas e utilizadas as primeiras redes de campo. No entanto, o trabalho de standardização só teve início em meados dos anos 80. A ideia básica de um *standard* é estabelecer uma especificação de uma forma muito rígida e formal, excluindo a possibilidade de pequenas alterações. Isto dá uma certa noção de confiabilidade e estabilidade da especificação, que por sua vez assegura a confiança dos utilizadores e consequentemente uma boa posição no mercado. Além disso, em muitos países os *standard*s têm uma posição *legally binding*, o que significa que quando um *standard* pode ser aplicado é obrigatório aplicá-lo. Isto implica que um sistema standardizado ganha uma posição competitiva em relação aos rivais não standardizados. Não é então de admirar que fosse iniciada uma corrida para a standardização.

A standardização internacional das redes de campo foi sempre difícil. Teve o seu início em 1985 e, depois de uns anos entusiásticos de desenvolvimento, a procura de um único *standard* foi ficando enredada numa rede de políticas de companhias e de interesses de *marketing* [7].

Na segunda parte dos anos 80, no início dos trabalhos da comissão técnica TC 65C do IEC (International Electrotechnical Commission) o desenvolvimento dos sistemas

fieldbus foi basicamente um projecto europeu, levado a cabo, não só por investigadores com um *background* académico, mas também por muitos proprietários. Os resultados mais promissores foram o francês FIP e o alemão PROFIBUS. Ambos foram standardizados a nível nacional e posteriormente propostos ao IEC para standardização internacional. No entanto, as abordagens dos dois sistemas eram completamente diferentes. O PROFIBUS baseava-se no controlo distribuído e a sua forma original suportava uma comunicação vertical orientada ao objecto, de acordo com o modelo cliente-servidor, no espírito da especificação MAP/MMS. Por outro lado, o FIP foi desenvolvido segundo um esquema de controlo centralizado mas capaz de suportar comunicação em tempo real, de acordo com o novo modelo para comunicação horizontal produtor-consumidor ou *publisher-subscriver*.

Como eram muito diferentes, os dois sistemas satisfaziam os requisitos de áreas de aplicação diferentes. Evidentemente, um *fieldbus* universal tinha de combinar os benefícios dos dois, pelo que um grupo de peritos apresentou uma nova proposta, o WorldFIP, que é uma extensão do FIP ao qual foi acrescentada a funcionalidade do modelo cliente-servidor. Por outro lado, o ISP (Interoperable System Project) tentou demonstrar que o PROFIBUS poderia ser melhorado com a introdução do modelo de comunicação *publisher-subscriber*. No entanto o ISP foi abandonado em 1994 por razões estratégicas [7].

Ao mesmo tempo, o papel de líder nos trabalhos de standardização ao nível do IEC foi sendo tomado, não pelos europeus, mas pelo comité SP50 do ISA (International Society of Automation), que foi muito mais eficiente no fim dos anos 80 e teve uma influência importante na estrutura de camadas do *standard* actual. No entanto, até meados dos anos 90 o comité do IEC não tinha produzido nenhum resultado substancial durante mais de 8 anos. A única excepção foi a definição da camada física, que foi adoptada como um *standard* IEC 61158-2 em 1993.

Em 1995, depois de longos anos de disputas entre investigadores alemães e franceses, com vista a combinar as abordagens FIP e PROFIBUS, várias companhias, basicamente americanas, decidiram não continuar a testemunhar as infindáveis discussões. Com o fim do projecto ISP, iniciaram a definição de uma nova rede de campo optimizada para a indústria de processos: o FF (Fieldbus Foundation). Este trabalho foi feito à parte dos comités IEC, dentro do ISA, e por algum tempo o trabalho no IEC pareceu posto de parte.

A 15 de junho de 1999 o comité de acção do IEC decidiu tomar um novo rumo e um mês depois, a 16 de Junho, os representantes das principais partes interessadas na

standardização *fieldbus* (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, PROFIBUS User Organization e Siemens) assinaram um "Memorando de Entendimento", com o objectivo de pôr um ponto final na disputa dos *standards fieldbus*.

Este processo culminou em 2003 com a adopção de uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 (Digital Data Communications for Measurement and Control - Fieldbus for use in Industrial Control Systems) e o IEC 61784 (Digital Data Communications for Measurement and Control - Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems), sendo ambos constituídos por um conjunto de perfis de comunicação, aos quais acabaram por corresponder as soluções comerciais mais importantes existentes à data da sua publicação (Tabela 2.1) [7].

Tabela 2.1 - Perfis e protocolos de acordo com o IEC 61784 e o IEC 61158

IEC 61784 Perfil	IEC 61158 Protocolos-camadas			Standard CENELEC	Nome comercial
	Física	Ligação de dados	Aplicação		
CPF-1/1	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H1)
CPF-1/2	Ethernet	TCP/UDP/IP	Tipo 5	-	Foundation Fieldbus (HSE)
CPF-1/3	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H2)
CPF-2/1	Tipo 2	Tipo 2	Tipo 2	EN-50170-A3	ControlNet
CPF-2/2	Ethernet	TCP/UDP/IP	Tipo 2	-	Ethernet/IP
CPF-3/1	Tipo 3	Tipo 3	Tipo 3	EN-50254-3	PROFIBUS-DP
CPF-3/2	Tipo 1	Tipo 3	Tipo 3	EN-50170-A2	PROFIBUS-PA
CPF-3/3	Ethernet	TCP/UDP/IP	Tipo 10	-	PROFINET
CPF-4/1	Tipo 3	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-485
CPF-4/1	Tipo 1	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-232
CPF-5/1	Ethernet	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS)
CPF-5/2	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS, subMMS)
CPF-5/3	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS)
CPF-6/1	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS
CPF-6/2	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS TCP/IP
CPF-6/3	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS Subset
CPF-7/1	Tipo 1	Tipo 6	-	-	Swiftnet transport
CPF-7/2	Tipo 1	Tipo 6	Tipo 6	-	Swiftnet full stack

Como se pode verificar pela tabela, sistemas *fieldbus* simples, como o CAN e o AS-*Interface*, não foram incluídos nesta norma. Estes estão incluídos num *standard* específico para este tipo de sistemas, o IEC 62026 (Low-voltage switchgear and controlgear - Controller-Device Interfaces), publicado em Junho de 2007.

À medida que o processo de standardização foi estabilizando, o desenvolvimento focou-se na definição de uma quarta camada, denominada camada de utilizador. O seu objectivo é disponibilizar ao utilizador uma abordagem integrada no desenvolvimento das aplicações, nomeadamente através da definição de blocos funcionais, linguagens de descrição dos dispositivos, interoperabilidade e métricas da qualidade de serviço.

Quanto ao seu posicionamento em relação aos níveis de controlo das aplicações industriais, as redes de campo sofreram uma evolução, passando também a ser utilizadas presentemente como redes de célula. A própria terminologia tem evoluído, através da definição de um conjunto de subcategorias para as redes de campo (Figura 2.7) [5]. Neste sentido, o termo original *fieldbus* tem sido utilizado para designar as redes de campo que estão mais próximas do conceito de rede de célula (ex. PROFIBUS-DP, WorldFIP) e o termo *sensorbus* para designar as redes mais básicas e mais próximas do conceito original de rede de campo (ex. AS-Interface, INTERBUS-S), enquanto o termo *devicebus* é utilizado para designar as que estão num plano de actuação intermédio (ex. DeviceNet, FF-H1). Contudo, e por uma questão de simplificação de linguagem, utiliza-se nesta dissertação apenas os termos rede de campo ou *fieldbus* para representar todas as subcategorias acima definidas.

Figura 2.7 - Categorias das redes de campo

2.6 Ethernet em Tempo Real

Ao mesmo tempo que decorria a standardização *fieldbus*, no mundo administrativo eram implementadas redes baseadas na Ethernet e no TCP/IP. Os custos associados a estas

infra-estruturas têm vindo continuamente a baixar e tornou-se possível ligar quase tudo, em qualquer lado do mundo, com a ajuda da tecnologia da Internet. No entanto, no campo da automação, ainda eram utilizados *fieldbuses* dedicados, a única barreira para aceder a componentes no chão de fábrica via Internet.

Depois de mais de 1 década de experiência com aplicações de *fieldbuses* a indústria começou a desenvolver e a adoptar soluções RTE. Os *standard*s propostos pelo IEC tentam traçar uma linha de orientação e critérios de selecção baseados em indicadores reconhecidos.

A adopção da tecnologia Ethernet na comunicação industrial pressupõe capacidades Internet, como por exemplo *interfaces* com o utilizador remotos, via Web. No entanto, é uma solução inaceitável se a adopção da tecnologia Ethernet causa perda de características necessárias no chão de fábrica, tais como [18]:

- Comunicação determinística;
- acções sincronizadas entre componentes e
- troca de pequenos pacotes de dados eficiente e frequente.

Um requisito implícito e essencial é a capacidade de comunicação Ethernet no nível de escritório ser totalmente absorvida, de modo que o *software* de comunicação envolvido possa ser utilizado. Isto resulta nos seguintes requisitos:

- Suporte de migração da Ethernet do nível do escritório para RTE e
- uso de componentes *standard* (*bridges*, controladores Ethernet e *stack*s de protocolo).

Para se obter a necessária alta qualidade de transmissão de dados, com *jitter* limitado e com perturbações devidas ao tráfego de dados TCP/IP limitadas é necessário desenvolver novos componentes de rede.

Resumindo, a RTE é uma especificação *fieldbus* que utiliza a Ethernet nos dois níveis mais baixos.

2.6.1 Standardização RTE

O *standard* Ethernet não atinge os requisitos do RTE. Existem diferentes propostas na comunidade de investigação para a modificação da tecnologia Ethernet. O mercado também adoptou soluções técnicas adicionais. A seguir são apresentadas as soluções RTE propostas para standardização.

As *interfaces* de comunicação estão estruturadas em diferentes níveis. Na figura 2.8 estão representadas as estruturas possíveis de um protocolo de comunicação RTE [18]. Comum a todas as redes Ethernet é a infraestrutura de cablagem universal.

As aplicações *non real time* utilizam os protocolos Ethernet, tal como definido no ISO 8802-3, e o protocolo TCP/UDP/IP. Utilizam ainda protocolos típicos da Internet, tal como o HTTP ou o FTP.

Figura 2.8 - Estruturas possíveis de uma RTE

Para uma solução RTE existem três diferentes abordagens:

- Na primeira mantêm-se os protocolos TCP/UDP/IP e a modificação que garante o tempo real é feita no nível mais alto. É a solução *on top of* TCP/IP.
- Na segunda não são utilizados os protocolos TCP/UDP/IP e a funcionalidade Ethernet é acedida directamente. É a solução *on top of Ethernet*.
- Na terceira abordagem o mecanismo Ethernet e a própria infraestrutura são modificados de forma a obter uma *performance* em tempo real. É a *Modified Ethernet*.

Na secção seguinte são apresentados os protocolos RTE que existem no mercado.

2.6.2 Protocolos RTE

O IEC 61784-2 (Industrial Communication Networks - Profiles – Part 2: Additional Fieldbus Profiles for Real time Networks based on ISO/IEC 8802-3) é o documento *standard* que especifica pelo menos dez diferentes soluções técnicas para RTE, sendo muitas delas incompatíveis [18] (Tabela 2.2). Alguns dos protocolos propostos apenas

estão definidos, não existindo ainda produtos no mercado. No caso de outros protocolos já existem produtos e aplicações.

Tabela 2.2 - Perfis RTE definidos no IEC 61784

Perfil IEC 61784	**Nomes comerciais**	***Ethertypes***
CPF-2	ControlNet (Ethernet/IP)	(0x0800 IP)
CPF-3	PROFIBUS/PROFINET	0x8892
CPF-4	P-NET	(0x0800 IP)
CPF-10	Vnet/IP	(0x0800 IP)
CPF-11	*TCnet* (Time Critical control network)	0x888B
CPF-12	EtherCAT	0x88A4
CPF-13	EPL (Ethernet PowerLink)	0x88AB
CPF-14	EPA (Ethernet for Plant Automation)	0x88BC
CPF-15	MODBUS – RTPS (Real Time Publisher Subscriber).	(0x0800 IP)
CPF-16	SERCOS (SErial Real time COmmunication System Interface)	0x88CD

Protocolos *on top of* TCP/IP

Algumas soluções RTE utilizam a *stack* do protocolo TCP/UDP/IP sem modificações. Com esta *stack* é possível comunicar de uma forma transparente para além dos limites da rede de campo.

É então possível implementar redes de campo que comuniquem com todos os pontos do mundo, da mesma forma que a tecnologia Internet. No entanto, o manuseamento desta *stack* de protocolo de comunicação requer recursos razoáveis, quer ao nível do processamento, quer ao nível da memória e introduz atrasos não determinísticos na comunicação.

A seguir são apresentadas algumas soluções disponíveis no mercado.

Modbus/TCP

Foi definido pela Schneider Electric e é mantido pela Modbus-IDA. Utiliza o já conhecido Modbus (o *standard* industrial “de facto” desde 1979) sobre uma rede TCP/IP, através da porta 502.

Esta é provavelmente uma das soluções Ethernet mais utilizadas em aplicações industriais e satisfaz os requisitos da classe mais baixa de aplicações, o controlo humano.

É um protocolo muito simples, do tipo *request/reply* (envia uma trama de *request* e recebe uma trama de *reply*). Em adição ao histórico Modbus, este protocolo tem definidas extensões *real time* que utilizam o RTPS. O RTPS prevê dois modelos de comunicação: o

publisher-subscriber, que transfere dados do *publisher* para o *subscriber*, e o CST (Composite State Protocol), que transfere informação de estado de um escritor para um leitor.

Ethernet/IP

Este protocolo foi definido pela Rockwell e é mantido pela ODVA (Open DeviceNet Vendor Association) e pela ControlNet International. Utiliza o CIP, que é comum nas redes Ethernet/IP, ControlNet e DeviceNet.

Este protocolo está incluído no *standard* IEC 61784-1 como CP 2/2 (tipo 2 no IEC 61158) e fornece comunicação *real time* baseada no ISO/IEC 8802-3.

Na Ethernet *full-duplex* não existe a possibilidade de atrasos devidos a colisões. No entanto, as tramas Ethernet podem sofrer atrasos no próprio dispositivo de *switch*, caso a porta de saída esteja ocupada na transmissão de outra trama. Isto pode levar a atrasos não determinísticos, que não são aconselháveis em aplicações em tempo real. Para evitar estes atrasos está definido um mecanismo de prioridades no IEEE 802.3, que permite a atribuição de níveis de prioridade (0 a 7) a tramas Ethernet.

P-NET

O P-NET sobre a especificação IP foi proposto pelo comité nacional dinamarquês e o seu uso destina-se ao ambiente IP. Neste protocolo a comunicação em tempo real P-NET é embebida em pacotes UDP/IP, que tanto podem circular em redes IP como em redes *non* IP.

Uma trama P-NET inclui uma tabela P-Net *route*, que por sua vez é constituída por dois elementos: os endereços da fonte e do destino da própria trama. No caso mais simples de uma rede de campo, estes são os endereços de dois nós da própria rede. Para permitir a comunicação entre dispositivos da rede de campo e dispositivos de uma rede IP os endereços da tabela P-Net *route* terão de ser endereços IP.

De facto, este protocolo apenas especifica a forma como são integradas redes P-NET e redes UDP/IP e não prevê nenhuma medida que assegure um comportamento em tempo real na rede Ethernet.

Vnet/IP

Este protocolo foi desenvolvido pela Yokogama.

Utiliza o TCP/IP para a integração de protocolos Internet, como o HTTP, e de extensões de protocolos *real time*, o RTP (Real Time and reliable datagram Protocol).

Este não é de facto um protocolo RTE, apenas utiliza o protocolo UDP/IP para o transporte do protocolo RTP. Não são tomadas nenhumas medidas especiais que garantam o comportamento determinístico de um protocolo *real time*.

Protocolos *on top of* Ethernet

Estes protocolos RTE não alteram o *hardware* de comunicação Ethernet, mas especificam um tipo de protocolo especial na trama Ethernet, o *Ethertype* (tabela 2.2). Por exemplo, o tipo *standard* para o protocolo IP é *Ethertype*=0X0800. Estes protocolos RTE utilizam, além da *stack* de protocolo IP *standard*, a sua própria *stack* de protocolo identificada com o seu próprio tipo. A tabela 2.2 lista os diferentes valores assignados para as várias soluções.

EPL

Foi definido por Bernecker & Rainer e é mantido pelo grupo de standardização EPL.

Baseia-se num sistema de escalonamento *master-slave* num segmento Ethernet partilhado, o SCNM (Slot Communication Network Management). O *master* é o MN (Managing Node), assegura o acesso em tempo real aos dados cíclicos e apenas permite a comunicação de tramas TCP/IP (*non real time*) em *slots* de tempo reservadas para este tipo de dados. Todos os outros nós são os CNs (Controlled Nodes) e apenas podem enviar dados a pedido do MN.

O ciclo de comunicação de um sistema EPL é composto por quatro períodos: *Start*, *Isochronous*, *Asynchronous* e *Idle* (Figura 2.9) [18]. No período *Start* o MN envia uma trama *multicast* SoC (Start of Cycle), que indica o início do ciclo. No período *Isochronous* o MN envia uma trama *unicast* PReq (Poll Request) para cada um dos CNs e o CN acedido envia uma trama *multicast* PRes (Poll Response). No início do período *Asynchronous* o MN envia uma trama SoA (Start of Asynchronous) e o acesso ao meio é permitido tanto ao MN como a qualquer CN, mas apenas pode ser enviada uma trama ASnd (ASynchronous data). O protocolo tipicamente usado neste período é o UDP/IP. Desta forma a transmissão de dados assíncronos nunca interfere com a transmissão de dados síncronos, o que garante um *timing* preciso na comunicação.

Figura 2.9 - Ciclo de comunicação do EPL

TCnet

É uma proposta da Toshiba. Tal como no EPL, a *interface* TCnet está entre a camada física e a camada de ligação de dados. O acesso MAC (Medium Access Control) típico da Ethernet, o CSMA/CD, é modificado.

O período de transmissão de alta velocidade é composto por um serviço de transmissão de dados cíclico em tempo real (no TCnet utiliza-se a expressão *time critical*) e por um serviço de transmissão assíncrona (no TCnet é denominada como *sporadic*) (Figura 2.10) [18].

Cada período de transmissão de alta velocidade é iniciado com o *broadcast* de uma trama SYN para todos os nós da rede. Depois de receber a trama SYN, o nó 1 inicia a transmissão das suas tramas de dados (DT). Quando termina faz o *broadcast* de uma trama CMP, que indica o fim da sua transmissão. Esta é recebida pelo nó 2, que inicia a transmissão das suas tramas de dados, repetindo-se o processo até ao último nó.

Figura 2.10 - Ciclo de comunicação do TCnet

EPA

O protocolo EPA é uma proposta chinesa.

Este protocolo permite uma comunicação determinística baseada num mecanismo de divisão de tempo dentro da camada MAC. O *macrocycle* (T) é o tempo total para completar um procedimento de transmissão de dados. Esse tempo é dividido em duas fases: a fase para transmissão de mensagens periódicas (Tp) e a fase para transmissão de mensagens aperiódicas (Tn) (Figura 2.11) [18].

A última parte de cada mensagem periódica é um anúncio de mensagem não periódica, que indica se o dispositivo que enviou a mensagem periódica tem ou não uma mensagem não periódica para transmitir. Se tiver, o dispositivo só a poderá enviar na fase Tn.

Figura 2.11 - Ciclo de comunicação do EPA

PROFINET CBA

Foi definido por um conjunto de vários fabricantes, incluindo a Siemens, e é mantido pela PROFIBUS Internacional.

A primeira versão foi baseada no CBA (Component Based Automation) e está incluída no IEC 61784-1 (tipo 10 no IEC 61158).

Para a transmissão de dados sem requisitos de tempo real é utilizada a *stack* TCP/IP e protocolos como o RPC (Remote Procedure Call) e o DCOM (Distributed Component Object Model). Quando é necessária comunicação em tempo real (para ciclos de tempo abaixo dos 100 ms) não é utilizada a *stack* TCP/IP, sendo preferido o protocolo em tempo

real, que é baseado no *Ethertype* 0x8892 e no mecanismo de atribuição de prioridade à trama.

Modified Ethernet

A topologia da cablagem típica da Ethernet é a topologia em estrela: todos os componentes estão ligados a um dispositivo central de *switch*.

Nas aplicações da área da automação, com a introdução do *fieldbus* a topologia em estrela foi substituída por topologias em barramento ou em anel para reduzir os custos na cablagem.

As soluções RTE devem estar preparadas, tanto para as topologias utilizadas no chão de fábrica, como para a topologia da *swicthed Ethernet*. Para isso existem duas soluções: ou a infraestrutura da rede de campo tem um *switch* para cada dispositivo, ou a funcionalidade de *switch* é integrada nos próprios dispositivos da rede de campo.

SERCOS

O SERCOS III é uma extensão RTE do SERCOS, definido pelo *standard* IEC 61491 (Electrical Equipment of Industrial Machines – Serial Data for Real-Time Communication for Controls and Drives), o seu processo de standardização teve início em 2005 e culminou em 2007 com a aprovação do *standard* IEC 61784-2/61158.

No sistema SERCOS existe uma estação *master* e estações *slave*s, cujo número pode variar entre 1 e 254. Todas as estações têm duas portas Ethernet. A topologia da rede pode ser *daisy-chain* ou em anel. Não são permitidos *switches* entre estações e, apenas no caso da topologia *daisy chain*, a porta Ethernet livre do último *slave* pode ser ligada a um *switch*, se for requerida comunicação entre dispositivos via TCP/IP ou UDP/UDP.

No sistema SERCOS III o ciclo de comunicação está dividido em dois períodos, denominados de canais de comunicação: o primeiro é o canal *real time* e o segundo, com menor duração, é o canal *non real time* (Figura 2.12) [18].

O ciclo de comunicação é iniciado pelo *master*, que envia a t*odos os slaves* dois tipos de telegramas *real time*: até 4 MDTs (Master Data Telegrams) e até 4 ATs (Answer Telegrams). Os MDTs contêm informação para sincronização, informação de controlo, dados de serviço do canal e valores de comando. Os ATs são transmitidos pelo *master* como uma trama vazia, mas com campos pré definidos, sendo cada um desses campos destinado a um determinado *slave*. Se um *slave* pretende enviar informação coloca-a no

seu campo e envia o telegrama AT. Quando termina o canal *real time* é iniciado o canal *non real time*, durante o qual podem ser enviados telegramas *non real time*.

Figura 2.12 - Ciclo de comunicação do SERCOS III

ETHERCAT

Este protocolo foi definido pela Beckoff e é mantido pelo grupo de tecnologia Ethercat (ETG). Utiliza as tramas Ethernet e uma topologia em anel especial.

Utiliza um mecanismo de acesso ao meio do tipo *master-slave*, no qual o nó *master* (tipicamente o sistema de controlo) envia tramas *Ethernet standards* ISO/IEC 8802-3 para os nós *slaves*, que por sua vez recebem e enviam dados através dessas tramas.

PROFINET IO

Este protocolo foi definido por vários fabricantes, sendo o mais importante a Siemens, e é mantido pela PROFIBUS Internacional.

Depois da definição PROFINET CBA, o passo seguinte foi a definição de um modelo de aplicação para o PROFINET IO baseado no PROFIBUS DP (tipo 3 do IEC 61158).

Num sistema deste tipo existem três tipos de dispositivos: os controladores IO, os dispositivos IO e o supervisor IO. Os controladores IO controlam os dispositivos IO com comunicação de dados cíclica através de um *buffer*. O supervisor IO gere o funcionamento dos componentes IO e dos controladores IO do sistema.

O ciclo de troca de dados entre os componentes de um sistema PROFINET IO é dividido nas seguintes fases de comunicação: IRT (Isochronous Real Time), RT (Real Time) e NRT (Non Real Time) (Figura 2.13) [18].

Na fase *Isochronous* a comunicação é escalonada no tempo: em cada tempo de offset a trama IRT é enviada de uma porta para outra sem interpretação do endereço por parte do switch. Nas fases seguintes os *switches* comportam-se como *switches standard* Ethernet, passando a comunicação a ser baseada no endereço. Primeiro são transmitidas as tramas RT durante a fase RT e quando esta termina é iniciada a fase NRT, durante a qual são transmitidas as tramas NRT.

Figura 2.13 - Ciclo de comunicação do PROFINET IO

2.7 Conclusão

Neste capítulo foram abordadas as redes de comunicação industriais, tendo sido feita uma análise aos principais protocolos actualmente utilizados.

Pode-se questionar sobre a necessidade do desenvolvimento de tantos protocolos. No entanto, tal facto é justificado, por um lado, pela pressão dos vários grupos económicos e, por outro, pela complexidade e variedade das possíveis áreas de aplicação.

Em relação a este segundo aspecto, é de facto difícil de conceber que uma única norma consiga abranger todas as áreas de aplicação e, nas várias tentativas feitas, provou-se que tal norma se tornava demasiado complexa, tendo um custo de implementação demasiado alto.

Quanto ao primeiro ponto, é evidente que as empresas fabricantes de sistemas e equipamento não tinham, e não têm, interesse em divulgar os protocolos de comunicação, para proteger os investimentos feitos em termos de I&D (Investigação e Desenvolvimento).

No entanto, depois de muitos anos de esforços foi adoptada uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 e o IEC 61784, que englobam as soluções comerciais mais importantes, incluindo soluções RTE.

Compete ao utilizador final e ao mercado decidir quais das soluções propostas preenchem os requisitos das aplicações em automação.

2 Redes de Comunicações Industriais

2.1 Introdução

A evolução da tecnologia nos últimos anos teve uma grande influência na sociedade, levando a caracterizá-la hoje como a sociedade do conhecimento. Com efeito, a globalização é hoje uma realidade, permitindo um rápido acesso à informação onde quer que ela se encontre, originando assim um esforço de actualização constante, já que a informação de que hoje dispomos ficará rapidamente ultrapassada.

O reflexo nas empresas fabris desta maneira de estar da sociedade actual traduz-se em novos desafios, no que respeita à produtividade: o nível de exigência do consumidor aumentou, os ciclos de vida dos produtos diminuíram, as linhas de produção tiveram de ser optimizadas em termos de níveis de *stocks* e flexibilidade, tudo a um baixo custo, para ser possível responder às necessidades do mercado de uma forma rentável. Este desafio nas áreas da inovação e da competitividade obrigou as empresas a concentrar esforços na modernização tecnológica dos seus processos de fabrico, nomeadamente na automatização dos mesmos. Deste esforço integrado resultaram, para além de produtos mais competitivos, o desenvolvimento de soluções tecnológicas avançadas que, à medida que se tornaram cada vez mais comuns e acessíveis, passaram também a ser incorporadas nos próprios processos de fabrico.

Durante as últimas três décadas assistiu-se a uma evolução sem paralelo na área dos sistemas de controlo, nomeadamente ao nível dos respectivos processos de concepção, implementação e operação. Isto deveu-se, em grande parte, aos novos desenvolvimentos, quer em áreas tecnológicas, tais como a microelectrónica e as telecomunicações, quer em áreas associadas à gestão e à integração de sistemas, bem como ao desejo de disponibilizar aos utilizadores finais equipamentos com maiores funcionalidades a custos mais reduzidos.

Este desenvolvimento reflectiu-se também ao nível das comunicações industriais, através da substituição progressiva das tradicionais comunicações ponto-a-ponto pelas

LANs (*Local Area Networks*). Embora inicialmente os motivos desta mudança estivessem relacionados com aspectos económicos, tais como a redução da cablagem e dos custos de manutenção, resultaram posteriormente em enormes vantagens ao nível da descentralização do controlo dos processos, na facilidade de instalação e configuração, na elevada flexibilidade de utilização e na melhoria do desempenho dos sistemas de controlo.

A crescente descentralização ao nível das funções de controlo e a crescente utilização de dispositivos inteligentes baseados em microprocessadores ou microcontroladores, criaram as condições necessárias para o desenvolvimento e proliferação das redes de campo. Estas são um tipo específico de rede local industrial, com o objectivo de interligar controladores, sensores e actuadores, que realizam a *interface* com o processo industrial.

Neste capítulo são analisadas as redes de comunicações industriais, com destaque para as redes de campo, os seus *standards* e as soluções comerciais ao nível das redes com fios. Neste contexto, na secção 1.2 é abordado o sistema de controlo do ambiente industrial, sendo ainda feito um resumo sobre a evolução das tecnologias de controlo. Na secção 1.3 é feita uma descrição do modelo OSI, uma vez que os *standards* de redes de campo são baseados nesse modelo. De seguida, na secção 1.4 é analisada a arquitectura das comunicações industriais, sendo ainda estabelecida uma relação entre esta e os níveis de controlo existentes num ambiente industrial. Na secção 1.5 são abordadas as redes de campo em particular, é feito um breve resumo sobre a história da standardização deste tipo de redes e são ainda apresentados os protocolos incluídos no conjunto de *standards* que especificam este tipo de redes. Por último, na secção 1.6 é abordada a *Ethernet* em tempo real e são apresentadas as soluções RTE (Real Time Ethernet) existentes.

2.2 O Sistema de controlo

O funcionamento de forma correcta e segura de um processo industrial de qualquer natureza é assegurado por intermédio de um sistema de controlo apropriado. Independentemente da dimensão ou da complexidade do processo em causa, o respectivo sistema de controlo pode ser decomposto em três subsistemas com funções bem definidas: o processo controlado, o controlador e o operador humano (Figura 2.1) [5].

Figura 2.1 - Sistema de controlo

O controlador é um equipamento que interage com o seu ambiente através de duas *interfaces* com características distintas:

- a *interface* com o processo controlado é definida como a *interface* de instrumentação;
- a *interface* com o operador humano é definida como a *interface* homem-máquina.
- A *interface* de instrumentação consiste num conjunto de sensores e actuadores que transformam os sinais físicos do processo controlado em sinais com características apropriadas para serem utilizados pelo controlador, e vice-versa. A *interface* homem-máquina consiste num conjunto de dispositivos de entrada e saída, que permitem a interacção com um operador humano. Tipicamente, esta interacção realiza-se ao nível da definição de parâmetros do processo e da supervisão da respectiva evolução.

A função do controlador é controlar a evolução do processo através da execução de um algoritmo de controlo adequado. A partir do processamento da informação obtida, quer directamente do estado do processo através da *interface* de instrumentação, quer fornecida pelo operador humano através da *interface* homem-máquina, o algoritmo de controlo produz um conjunto de comandos que são enviados para o processo através da *interface* de instrumentação. Para realizar estas funções o controlador dispõe de uma estrutura funcional, baseada na utilização de equipamentos adequados ao processo em causa, que suporta a execução do algoritmo de controlo.

Ao nível da estrutura funcional, estes sistemas de controlo podem ser classificados em três tipos de arquitecturas (Figura 2.2) [5].

- Centralizadas - o algoritmo de controlo é executado por um único equipamento;
- Descentralizadas - o algoritmo é executado num único equipamento, mas

algumas tarefas de processamento mais simples (ex. condicionamento e aquisição de sinais) são executadas por outros equipamentos de menor complexidade. Isto implica a existência de uma estrutura de comunicações que permita a interacção e a cooperação entre os vários equipamentos (ex. comunicações série ponto-a-ponto);

- Distribuídas - o algoritmo de controlo encontra-se distribuído por vários equipamentos de complexidade e natureza distintas. Tal como nas arquitecturas descentralizadas, é também necessário dispor de uma estrutura de comunicações adequada, sendo esta, contudo, comparativamente muito mais complexa (ex. rede de campo).

Figura 2.2 - Exemplos de arquitecturas de controlo

2.2.1 Evolução das Tecnologias de Controlo

O advento do computador no início dos anos 60 permitiu que estes passassem também a ser utilizados para implementar funções de controlo. O termo DCC (Direct Digital Control) foi utilizado na época para enfatizar o facto do controlo do processo ser realizado directamente pelo computador. O facto de serem programáveis proporcionou-lhes uma esmagadora vantagem em comparação com as tecnologias de lógica discreta utilizadas até ao momento. Um único equipamento (um computador) concentra em si, quer

as tarefas do controlador, quer as *interfaces* de instrumentação e de homem-máquina. No caso da *interface* de instrumentação, os sensores e actuadores são tipicamente ligados ao controlador através de ligações ponto-a-ponto analógicas (ex. anel de corrente). Em paralelo com este processo, tem também início nos finais do anos 60 o desenvolvimento de máquinas de controlo numérico e de *robots* industriais.

As arquitecturas de controlo desenvolvidas até esta época são essencialmente centralizadas. Contudo, as crescentes exigências da indústria, conjugadas com o desenvolvimento do microprocessador no início dos anos 70, permitiram uma evolução para as primeiras arquitecturas descentralizadas. Esta evolução efectuou-se segundo duas perspectivas [6]:

- uma ao nível das indústrias de processos, com o desenvolvimento dos DCS (Distributed Control Systems) com o objectivo de interligar hierarquicamente os equipamentos de controlo de menor complexidade (por exemplo controladores PID - Proportional Integral Derivative) aos equipamentos de maior complexidade (por exemplo mini-computadores);
- outra ao nível das indústrias de manufactura, onde o PLC, cujo desenvolvimento se deu no início dos anos 70, foi utilizado como elemento central das arquitecturas de controlo.

Em ambas as perspectivas, a interligação entre equipamentos era tipicamente realizada, quer através de ligações ponto-a-ponto analógicas, quer através de ligações digitais, utilizando neste último caso protocolos de comunicação proprietários. Embora esta evolução tenha permitido o desenvolvimento de sistemas de controlo cada vez mais complexos, durante a primeira década da sua utilização, as arquitecturas de controlo continuaram a ser caracterizadas por uma estrutura tipicamente centralizada e só mais tarde se registou uma evolução para soluções do tipo descentralizado.

Entre meados dos anos 80 e inícios dos 90, assistiu-se a uma alteração da estrutura das arquitecturas de controlo através da crescente utilização de redes de comunicação industriais para interligar os equipamentos de controlo. Esta evolução tecnológica foi o ponto de partida das primeiras arquitecturas de controlo descentralizadas baseadas numa estrutura de comunicações digital. Estas arquitecturas, embora mais complexas, permitiram obter um importante conjunto de vantagens, das quais se destacam: menores custos, melhores desempenhos, instalação e manutenção mais simples, modularidade, facilidade

na detecção de erros e avarias, etc. Na sequência desta evolução, surge também nesta época o conceito de CIM (Computer Integrated Manufacturing).

O CIM visa a cooperação entre os diferentes sistemas intervenientes no ambiente de fabrico e engloba todas as actividades com ele relacionadas, desde o projecto e desenvolvimento até ao *marketing* e vendas, passando pelo controlo do fabrico. Para que essa cooperação exista de facto é necessário que haja integração entre os sistemas. A integração significa a possibilidade de os subsistemas da empresa poderem interactuar entre si através de sistemas de comunicações de dados e bases de dados comuns.

Os sistemas de comunicações requerem infraestruturas técnicas (*software* e *hardware*). As comunicações requerem também regras (protocolos), regras essas condicionadas, não apenas por aspectos técnicos, mas também pela funcionalidade exigida.

Uma das representações da filosofia CIM consiste em decompor a empresa em cinco níveis, tal como a figura 2.3 indica.

Figura 2.3 - Representação da filosofia CIM

A subdivisão em níveis é baseada, entre outros aspectos, nos tipos de actividades realizadas na empresa e leva, geralmente, ao uso de diferentes tipos de redes de comunicações nos vários níveis.

No interior de cada nível as comunicações horizontais são geralmente asseguradas por uma rede local. As comunicações verticais entre dois níveis adjacentes são resolvidas interligando as redes através de dispositivos de ligação.

A figura 2.4 representa um exemplo de uma arquitectura possível para a hierarquia de comunicações dentro de uma empresa.

Nos níveis superiores da hierarquia as comunicações podem ser caracterizadas como correspondendo à troca de grandes quantidades de informação, que tem de ser processada durante períodos relativamente longos mas com uma frequência relativamente baixa.

Ao contrário, nos níveis inferiores da hierarquia pequenas quantidades de informação precisam de ser processadas de uma forma rápida, com o objectivo de controlar processos industriais em tempo real. Este tipo de transacções tem normalmente uma periodicidade cíclica e uma frequência relativamente elevada.

Pode-se então concluir que não é possível satisfazer todos estes requisitos de transferência de dados com um só tipo de rede.

Figura 2.4 - Representação de uma arquitectura possível para a hierarquia das comunicações de uma empresa

Pode assim propor-se uma classificação hierárquica das comunicações industriais em três grandes grupos, que são: redes de fábrica, redes de célula e redes de campo.

As redes de fábrica abrangem os níveis superiores da hierarquia, enquanto as redes de campo correspondem ao nível mais baixo.

Embora esta evolução abrisse um conjunto enorme de perspectivas ao nível da integração de equipamentos situados em diferentes níveis de controlo, na prática isto acabou por não se verificar, devido ao desenvolvimento de muitas soluções proprietárias. Estas acabaram por limitar as potencialidades das arquitecturas de controlo, nomeadamente

ao nível da integração e da interoperabilidade entre equipamentos. Este problema colocou-se de forma especialmente grave ao nível das redes de campo, com os diferentes fabricantes a tentar impor as suas soluções como o *standard* a utilizar. São alguns exemplos o (PROcess FIeld BUS), o WorldFIP (Factory Instrumentation Protocol), o DeviceNet, o INTERBUS-S, e o AS-Interface (Application Server). Este processo terminou apenas recentemente através da adopção de uma solução de compromisso entre as várias propostas existentes [7]. Ao nível das arquitecturas de controlo registou-se uma tendência para adoptar soluções distribuídas, não só devido à possibilidade de dispor de equipamentos com maiores capacidades de processamento, mas também através do desenvolvimento de arquitecturas de comunicação que suportam elevados níveis de integração entre equipamentos.

Embora a introdução das redes industriais viesse resolver o problema da integração horizontal de equipamentos (situados no mesmo nível de controlo), a integração vertical (entre níveis de controlo) foi sempre um problema em aberto. As soluções apontadas inicialmente passavam pela utilização de equipamentos dedicados (*gateways*) ou pelo desenvolvimento de *software* específico que implementava as tarefas de mapear os serviços de comunicação das diferentes redes. Como estas soluções eram normalmente caras e complexas, surgiu no final dos anos 80 a ideia de desenvolver uma arquitectura de comunicações aberta baseada na estrutura do modelo OSI (*Open Systems Interconnection*). Exemplos destas soluções foram o MAP (Manufacturing Automation Protocol) e o MMS (Manufacturing Message Specification). No entanto, o seu sucesso acabou por ser limitado devido, quer à falta de suporte tecnológico adequado, quer à cumplicidade das soluções propostas.

Em paralelo, nas indústrias de processos a utilização de tecnologias SCADA (Supervisory Control and Data Aquisition) foi vista como uma alternativa mais simples e razoavelmente eficaz na integração vertical. Contudo, devido, quer à ausência de adequação destes sistemas para o problema em causa, quer à proliferação de equipamentos de controlo com características muito diversas, a utilização desta tecnologia acabou por resultar em soluções bastante limitadas.

Nos finais dos anos 90, devido às crescentes exigências de integração com aplicações de nível intermédio e superior, nomeadamente o ERP (Enterprise Resource Planning) e o MES (Manufacturing Execution System), foram desenvolvidas um conjunto de tecnologias de *software* baseadas em plataformas de objectos distribuídos, que disponibilizavam uma

infraestrutura ao nível dos serviços de comunicações, permitindo assim desenvolver de forma eficaz os conceitos de integração vertical e horizontal. São exemplos destas tecnologias o CORBA (Common Object Request Broker Architecture), com uma gama alargada de domínios de aplicação, e o OPC (Object linking and embedding for Process Control), que foi especialmente desenvolvido para satisfazer os requisitos no domínio das aplicações industriais. Este processo apresenta actualmente uma grande dinâmica, com destaque para o desenvolvimento de *standards* com base em arquitecturas de objectos distribuídos especialmente vocacionados para as necessidades dos ambientes industriais: IEC 61499 (Function Blocks for Industrial-Process Measurement and Control Systems) e o IEC 61804 (Function Blocks for Process Control). Como resultado deste trabalho, as arquitecturas de comunicação mais recentes já incorporam muitas destas funcionalidades, das quais se destacam: o CIP (Common Industrial Protocol), o IDA (Interface for Distributed Automation), o HSE *fieldbus* (High Speed Ethernet) e o PROFINET.

Entre os finais dos anos 90 e o início da corrente década verificou-se um fenómeno de migração de tecnologias de uso geral para a área das comunicações industriais. O caso mais paradigmático deu-se com a utilização da rede Ethernet em ambientes industriais (IE - Industrial Ethernet). Este processo teve um profundo impacto na estrutura das comunicações industriais, afectando todos os níveis de controlo. Esta migração deveu-se a vários factores, tais como: a existência de soluções de *hardware* de baixo custo e de elevado desempenho, bem como de protocolos de comunicação abertos e a disponibilização de plataformas de *software* para o desenvolvimento integrado de aplicações distribuídas.

A etapa mais recente desta evolução está centrada na utilização das tecnologias desenvolvidas para Web, tais como UDP/TCP/IP (User Datagram Protocol / Transmission Control Protocol / Internet Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), XML (eXtensible Markup Language), Proxys, Java, ou Jini, para o desenvolvimento de aplicações industriais. A utilização destas tecnologias, para além de estarem largamente difundidas e do seu custo reduzido, vai permitir obter níveis de integração superiores nomeadamente ao nível dos domínios de aplicação externos ao ambiente industrial [11].

Associado ainda a este processo de migração de tecnologias emergentes para as redes industriais, é de salientar a crescente tendência para a utilização de redes de comunicações sem fios (como o IEEE 802.11 ou o IEEE 802.15) em ambientes industriais [9], [10].

2.3 O Modelo de Referência OSI

Convém agora, fazer uma descrição do modelo OSI, uma vez que os protocolos de comunicações industriais a seguir mencionados têm como referência esse modelo.

Num ambiente onde existem equipamentos provenientes de diferentes fabricantes a integração implica a definição de protocolos de comunicação normalizados. A ISO (International Organization for Standardization) definiu o modelo de referência OSI com o objectivo de promover o aparecimento de normas na área das comunicações entre computadores, equivalente ao que na altura se verificava já para as comunicações telefónicas, definidas no âmbito da CCITT (Commité Consultatif International de Telegraphique et Telephonique) [12]. O termo "sistema de arquitectura aberta" indica que se um sistema estiver conforme com o modelo OSI então está aberto a comunicar com qualquer outro que obedeça às mesmas normas. É de salientar que o modelo de referência OSI não especifica por si as normas de comunicação. O seu propósito é apenas fornecer uma arquitectura que sirva de base ao desenvolvimento de normas para sistemas de comunicação.

O modelo de referência OSI define 7 camadas, conforme se indica na figura 2.5.

Figura 2.5 - O modelo de referência OSI

A hierarquia dos níveis vai subindo, desde o nível de maior especificidade até ao mais alto, que é o nível mais genérico.

Os três primeiros níveis fornecem um serviço de rede, ou seja, tratam do transporte da informação. O nível físico trata do meio físico para a transmissão de *bits* de informação, o nível lógico organiza os *bits* de uma forma ordenada em blocos (tramas) e assegura que eles são transmitidos e recebidos de uma forma correcta, enquanto o nível de rede assegura que os pacotes chegam ao seu destino final.

Enquanto o serviço de rede fornecido pelos três níveis inferiores é adequado para transportar informação, algumas aplicações podem ter especificações que as redes não fornecem, como por exemplo uma taxa de erros baixa, um elevado nível de segurança, ou a necessidade de manter uma sequência de pacotes que façam uma mensagem completa. São estes os serviços que o nível de transporte fornece aos níveis superiores.

Os níveis acima do nível de transporte não tratam de mecanismos de transmissão de informação. Esse é o trabalho dos quatro níveis inferiores. No entanto, a informação necessita de ser sincronizada e tratada para que as aplicações entendam. O nível de sessão fornece o serviço de gestão da comunicação entre aplicações.

Outro ponto importante é o formato em que a informação é trocada. Os dois sistemas que estão a comunicar podem ter maneiras diferentes de representar os dados. O nível de apresentação preenche o requisito de identificar e estabelecer uma sintaxe comum, que será utilizada pelos dois sistemas.

O nível mais alto é o nível de aplicação, que constitui a *interface* entre as aplicações propriamente ditas e o sistema de comunicações.

Tendo sido feita uma introdução do modelo, a seguir é feita uma abordagem mais detalhada, especificando, em cada nível: os seus objectivos, os serviços oferecidos ao nível imediatamente superior e as suas funções.

2.3.1 O Nível Físico

O nível físico é responsável por uma transmissão transparente da informação através do meio físico. As funções do nível físico são inteiramente independentes do meio físico em uso, seja este constituído por fio de cobre, cabo coaxial ou fibra óptica. O tipo de meio físico utilizado é completamente escondido ao nível lógico pelo nível físico.

As definições do nível físico podem ser agrupadas da seguinte forma:

- Mecânicas: definem o tipo de conector, as dimensões físicas, as posições dos

pinos, etc;

- Eléctricas: definem as características eléctricas, como por exemplo: níveis eléctricos, impedância, etc;
- Funcionais: definem qual o significado dos níveis eléctricos em determinados pinos do conector;
- Procedimentais: definem as regras (procedimentos) a aplicar às várias funções e também qual a sequência em que determinados eventos podem ocorrer.

Serviços Fornecidos ao Nível Lógico

O nível físico fornece os seguintes serviços ao nível lógico:

- Ligações físicas: o fornecimento de uma transmissão de *bits* perfeitamente transparente entre entidades lógicas. A ligação física estabelece um "circuito de informação" entre dois pontos. A ligação física pode ser estabelecida entre dois pontos ou directamente, ou através de um sistema intermédio;
- Tratamento das unidades de informação: este serviço compreende a transmissão de um *bit* em transmissão série, ou de n *bits* em transmissão paralela. A ligação física pode ser *full-duplex* (a informação é feita nos dois sentidos simultaneamente), *half-duplex* (a informação é feita nos dois sentidos mas alternadamente), ou ainda *simplex* (a informação só é feita num sentido);
- Ligação entre pontos: a ligação entre pontos pode ser ponto-a-ponto ou multiponto;
- Sequenciamento: o nível físico coloca os *bits* no meio físico na mesma ordem que lhe foram fornecidos pelo nível lógico
- Identificação de circuito: o nível físico fornece identificadores que definem univocamente a ligação entre dois sistemas. O nível físico fornece identificadores da ligação entre pontos, que podem ser utilizados pelo nível lógico;
- Recuperação de falhas: o nível lógico é notificado de problemas detectados pelo nível físico;
- Parâmetros fornecidos ao nível lógico: são fornecidos parâmetros ao nível lógico, tais como: taxas de erro, taxas de transmissão, disponibilidade de serviço e atrasos.

Funções do Nível Físico

As seguintes funções são executadas pelo nível físico:

- Estabelecimento e libertação das ligações entre entidades do nível lógico;
- Transmissão de sequências de *bits*: estas podem ser síncronas ou assíncronas;
- Gestão: os protocolos do nível físico tratam de alguns aspectos relacionados com a gestão das actividades deste nível.

2.3.2 O Nível Lógico

O nível lógico isola os níveis superiores das características do meio de transmissão e fornece uma ligação sem erros e de confiança. O nível lógico é estabelecido sobre uma ou mais redes físicas e liga duas identidades em sistemas adjacentes. As ligações lógicas são ponto-a-ponto.

Dentro do nível lógico as sequências de *bits* do nível físico são organizadas em blocos de informação denominados tramas. São funções do nível lógico a sincronização dos *bits* dentro de uma trama, a detecção e correcção de erro (através da retransmissão de pacotes) e ainda o controlo de fluxo (dependendo do estado do sistema de recepção, liga ou desliga a transmissão de pacotes).

Serviços Fornecidos ao Nível de Rede

Os seguintes serviços são fornecidos pelo nível lógico:

- Ligação lógica: o estabelecimento de uma ou mais ligações entre duas entidades;
- Unidades de informação do nível lógico: estas entidades teóricas são mapeadas numa base de uma para uma em unidades do protocolo em uso. Na prática, estas são as tramas transmitidas numa ligação lógica;
- Identificadores lógicos: se requerido pelo nível físico, o nível lógico pode fornecer identificadores dos pontos da ligação lógica;
- Sequenciamento: manutenção da sequência correcta de pacotes;
- Detecção de erros: se for detectado um erro não recuperável pelo nível lógico, então o nível físico será notificado;
- Controlo de Fluxo: o nível de rede pode controlar dinamicamente a taxa a que pode receber os pacotes;
- Parâmetros da qualidade do serviço: estes parâmetros são opcionais e incluem

tempos médios entre erros detectados mas irrecuperáveis, taxa de erro residual, disponibilidade do serviço e débito.

Funções do Nível Lógico

As seguintes funções são efectuadas no nível lógico:

- Estabelecimento e libertação das ligações do nível lógico: como foi referido, esta função faz um mapeamento das unidades de informação em unidades do protocolo, em uso numa forma de uma para uma;
- Separação de ligações lógicas: esta função é feita dividindo uma ligação lógica em várias ligações físicas;
- Delimitação e sincronização: esta é essencialmente uma função de empacotamento, que organiza *bits* (unidades do nível físico) em tramas (unidades lógicas);
- Controlo de sequência: mantém a ordem sequencial dos pacotes transmitidos através da ligação lógica;
- Detecção de erros: esta função detecta erros de transmissão, de formato e de operação, que usualmente aparecem devido a deficiências no meio físico;
- Recuperação de erros: esta função tenta recuperar os erros, geralmente através da retransmissão de pacotes;
- Controlo de fluxo: fornece os serviços de controlo de fluxo já descritos;
- Identificação e troca de parâmetros: efectua a identificação de entidades lógicas e controla a troca de parâmetros;
- Controlo da ligação do circuito de dados: esta função fornece o nível de rede com a informação necessária para controlar e manter o circuito de dados ao nível de rede;
- Gestão: os protocolos do nível físico tratam de alguns aspectos da gestão das actividades deste nível.

2.3.3 O Nível de Rede

A função essencial do nível de rede é fornecer uma transmissão de dados perfeitamente transparente de um nível de transporte de um sistema (por exemplo uma aplicação num terminal) a um nível de transporte de outro sistema (por exemplo a aplicação servidora num computador central).

Em redes complexas, entidades comunicantes no nível de transporte não necessitam de estar próximas, mas ligadas através de um ou mais sistemas intermédios. Nestes casos, o nível de rede fornece funções de encaminhamento. Um exemplo pode ser a ligação de uma rede pública de dados com uma rede privada (por exemplo uma rede bancária) e uma rede local. Os endereços de rede são utilizados para identificar as várias entidades comunicantes no nível de transporte ao nível de rede.

Serviços Fornecidos ao Nível de Transporte

Os seguintes serviços são fornecidos pelo nível de rede:

- Endereços de rede: são fornecidos pelo nível de rede e são usados por entidades do nível de transporte, de forma a identificar univocamente outras entidades do nível de transporte;
- Ligações de rede: fornecem os meios de transferir dados entre entidades do nível de transporte;
- Identificadores de Ligações Rede entre sistemas: o nível de rede fornece às entidades do nível de transporte um identificador de ligação associado univocamente com o endereço de rede;
- Unidades de informação do nível de rede: numa ligação de rede o nível de rede fornece, para transmissão, unidades de informação (pacotes de dados). Estas unidades têm um cabeçalho e um final perfeitamente definidos. A integridade da unidade é verificada no nível de rede;
- Parâmetros de qualidade do serviço: estes parâmetros incluem taxa residual de erros, disponibilidade do serviço, habilidade, débito, atraso no tráfego e atraso no estabelecimento de ligações na rede;
- Notificação de erros: erros irrecuperáveis para o nível de rede são participados ao nível de transporte;
- Sequenciamento: o nível de rede pode fazer a entrega de unidades de informação do nível de rede sequencialmente para uma determinada ligação de rede;
- Controlo de fluxo: a entidade de transporte que está a receber pode fazer com que o Serviço de Rede pare de enviar mais unidades de informação. Este controlo de fluxo pode ou não ser enviado ao outro extremo da ligação;
- Libertação: a entidade de transporte pode pedir a libertação da ligação.

Funções do Nível de Rede

As funções de nível de rede fornecem uma grande variedade de configurações, desde ligações ponto-a-ponto a ligações mais complexas, com uma combinação de várias sub-redes. As seguintes funções são efectuadas:

- Encaminhamento e repetição: as ligações da rede são fornecidas por entidades nos sistemas finais, mas podem ser envolvidas entidades em sistemas intermédios que façam repetição. As funções de encaminhamento determinam um caminho definido entre dois endereços;
- Ligações de rede: esta função fornece ligações entre entidades do nível de transporte, fazendo uso de ligações fornecidas pelo nível lógico;
- Multiplexação de ligações de rede: esta função é usada para multiplexar ligações de rede em ligações lógicas;
- Segmentação e empacotamento: o nível de rede pode segmentar e/ou formar blocos que constituem unidades de informação do nível de rede, para facilitar o transporte;
- Funções de detecção de erros: são utilizadas para verificar se a qualidade dos serviços fornecidos numa rede é mantida. Quando há detecção de erros no nível de rede o nível lógico é notificado. As funções de recuperação de erros dependem da qualidade do Serviço de Rede fornecido;
- Sequenciamento: prevê a entrega sequencial de unidades de informação do Serviço de Rede numa determinada ligação;
- Controlo de fluxo;
- Selecção de serviços: esta função permite que sejam seleccionadas as mesmas funções nos dois sistemas, mesmo quando a ligação se faz entre vários subsistemas.

2.3.4 O Nível de Transporte

O papel do nível de transporte é complementar a rede que está por baixo, de forma a assegurar a qualidade dos serviços requeridos que estão acessíveis ao utilizador.

As funções do nível de transporte estão focalizadas em optimização de custos, controlo de erros, controlo de fluxos, sequenciamento e multiplexagem. O nível de transporte também verifica a existência de duplicados e perdas de informação. Se a ligação de rede for quebrada temporariamente, a ligação de transporte pode ser mantida até que a ligação seja restaurada.

Os protocolos do nível de Transporte são definidos para aceitar uma grande variedade de redes, com várias qualidades de serviços. São cinco as classes de Serviços de Transporte disponíveis:

- A classe 0 é a classe mais simples, sem melhoramentos nos Serviços de Rede;
- A classe 1 adiciona recuperação de erros para redes sujeitas a uma grande frequência de interrupções;
- A classe 2 tem as funções da classe 0 mais multiplexagem;
- A classe 3 tem as funções da classe 1 mais multiplexagem;
- A classe 4 adiciona funções de detecção de erros e de dados fora de sequência.

Serviços Fornecidos ao Nível de Sessão

Os seguintes serviços são fornecidos pelo nível de transporte:

- Estabelecimento de ligações de transporte: as ligações de transporte são estabelecidas entre identidades do nível de sessão e são identificadas pelo endereço de transporte. A qualidade do serviço é negociada entre as entidades do nível de sessão e o serviço de transporte;
- Transferência de dados: fornece a transferência de dados, de acordo com a qualidade de serviço que foi negociada;
- Libertação da ligação de transporte: fornece meios para que qualquer entidade da camada de sessão dos sistemas possa libertar a ligação de transporte.

Funções do Nível de Transporte

As operações no nível de transporte são:

1 Fase de Iniciação

Durante esta fase são efectuadas as seguintes funções:

- Obtenção de uma ligação à rede que corresponda aos requisitos em termos de custos e qualidade de serviço.
- Decisão de multiplexagem ou divisão.
- Estabelecer as unidades de informação do protocolo de transporte óptimas.
- Selecção das funções que devem estar operacionais durante a transferência de dados.
- Mapeamento dos endereços de transporte em endereços de rede.

- Fornecimento de identidade aos endereços de transporte.
- Transferência dos dados.

2 Fase de Transferência

Durante esta fase é executada a transmissão de unidades de informação do protocolo de transporte. Os seguintes serviços podem ser usados ou não, dependendo da classe de serviço seleccionada:

- Sequenciamento;
- Empacotamento;
- Segmentação;
- Multiplexagem ou divisão;
- Controlo de fluxo;
- Detecção e recuperação de erros;
- Transferência dos dados enviados;
- Delimitação das unidades de informação do serviço de transporte;
- Identificação das ligações de transporte.

3 Fase de Libertação

Esta fase inclui as seguintes funções:

- Notificação das razões da libertação.
- Identificação da ligação de transporte libertada.
- Transferência de dados.

2.3.5 O Nível de Sessão

Os requisitos para o nível de sessão reflectem a observação da utilização dos sistemas, pela maior parte dos utilizadores, em picos de actividade que podem ser chamados de sessões. Durante a sessão, o utilizador e o sistema iniciam um diálogo. A primeira função do nível de sessão é estabelecer, manter e gerir este diálogo.

As ligações da camada de Sessão são mapeadas em ligações da camada de transporte numa razão de um para um. Não existe multiplexagem neste nível, mas é possível que várias ligações de sessão usem a mesma ligação de transporte sequencialmente. Simultaneamente, uma ligação de sessão pode usar mais que uma ligação de transporte. Se a ligação de transporte se quebrar, devido a problemas nas camadas inferiores da rede, é possível estabelecer uma nova ligação de transporte sem a intervenção do utilizador ou

mesmo chegar ao seu conhecimento a quebra. Neste caso é o nível de sessão que é o responsável pela ressincronização do diálogo entre os dois sistemas.

Serviços Fornecidos ao Nível de Apresentação

Os seguintes serviços são fornecidos pelo nível de sessão:

- Estabelecimento da ligação entre níveis de sessão: permite que duas entidades do nível de apresentação possam estabelecer uma ligação de sessão entre elas;
- Libertação de ligação: permite que entidades do nível de apresentação possam libertar uma ligação do nível de sessão de uma forma ordeira e sem perda de informação;
- Transferência de dados: permite que uma entidade emissora do nível de apresentação possa transferir uma unidade de informação do nível de sessão a uma entidade receptora do nível de apresentação;
- Serviço de Quarentena: permite à entidade emissora solicitar que algumas unidades de informação, enviadas por uma conexão do nível de sessão, não devam ser enviadas à entidade receptora do nível de apresentação, até ordem contrária enviada pelo emissor;
- Gestão de Interacção: permite que entidades do nível de apresentação comandem explicitamente quem vai controlar certas funções de controlo. São possíveis os seguintes tipos de interacção: dois sentidos simultaneamente, dois sentidos alternadamente, um sentido;
- Sincronização de ligação: este serviço permite que entidades do nível de apresentação definam e identifiquem pontos de sincronização que obriguem uma ligação do nível de sessão a permanecer num determinado estado (*reset*) e que definam qual o ponto de ressincronização;
- Situações excepcionais: faz a notificação ao nível superior de quaisquer situações não englobadas pelos serviços deste nível.

Funções do Nível de Sessão

A maior parte das funções necessárias neste nível estão implícitas aos serviços deste nível:

- Mapeamento das ligações de sessão às ligações de transporte;
- Controlo do fluxo do nível de sessão: o nível de sessão não possui controlo de fluxo. Para evitar aumentar as funções do nível de sessão este controlo é feito no nível de

transporte;

- Recuperação de ligações quebradas: no caso de quebra de ligação do nível de transporte o nível de sessão pode ter as funções necessárias para restabelecer uma nova ligação, de forma a continuar a sessão;
- Libertação da ligação de Sessão: permite que se acabe e liberte a ligação sem perda de informação.

2.3.6 O Nível de Apresentação

Este nível é responsável por assegurar que a informação é apresentada ao utilizador de uma forma útil (através do nível de aplicação). O nível de apresentação só trata da sintaxe da informação (a forma como é representada a informação) e não com a sua semântica (significado da informação).

Serviços Fornecidos ao Nível de Aplicação

Os seguintes serviços são fornecidos pelo nível de apresentação:

- Transformação da Sintaxe: trata dos códigos e do conjunto de caracteres a usar (por exemplo o código ASCII), bem como da apresentação da informação (por exemplo a visualização da informação num monitor);
- Selecção da Sintaxe.

Funções do Nível de Apresentação

As funções do nível de apresentação são:

- Negociação e Renegociação da Sintaxe;
- Transformação da Sintaxe;
- Gestão da passagem de serviços dos Níveis Sessão e Aplicação.

2.3.7 O Nível de Aplicação

O nível de apresentação constitui o *interface* entre as aplicações propriamente ditas e o sistema de comunicação. As aplicações trocam informação entre si, utilizando entidades e protocolos do nível de aplicação e serviços do nível de apresentação.

Serviços Fornecidos às Aplicações

Além da transferência da informação, estes serviços podem incluir:

- Identificação dos vários intervenientes da comunicação através do nome, endereço e descrição;
- Determinação da disponibilidade dos intervenientes;
- Verificação e validação dos intervenientes;
- Determinação dos recursos necessários;
- Determinação da qualidade de serviço mínima;
- Sincronização de aplicações;
- Selecção da forma de diálogo;
- Entendimento na responsabilidade na recuperação de erros;
- Acordo na forma de controlo da integridade da informação;
- Identificação de limitações na sintaxe da informação.

Funções do Nível de Aplicação

O nível de aplicação contém todas as funções exigidas pela comunicação entre sistemas abertos, mas que não são fornecidas pelos níveis inferiores. As comunicações entre aplicações são efectuadas através de entidades do nível de aplicação. Estas entidades representam conjuntos de capacidades de comunicação OSI e estão divididas em elementos específicos implementados pelo utilizador e elementos pertencentes aos serviços do nível de aplicação, sendo estes últimos denominados por ASE (Application Service Element).

Um exemplo de um serviço do tipo ASE é o MMS (Manufacturing Message Specification), que é uma norma internacional do nível de aplicação vocacionada para o ambiente industrial.

2.4 A Arquitectura das Comunicações Industriais

Ao nível dos sistemas de controlo a integração implica a necessidade de cooperação e interacção entre os vários subsistemas incluídos no mesmo sistema. Isto significa transferência, armazenamento e processamento de informação em ambientes com características heterogéneas, o que por sua vez obriga à necessidade de dispor de uma infra-estrutura de comunicações adequada. As redes locais industriais, não sendo a solução para este problema, são contudo uma parte integrante e essencial dessa solução.

Os fluxos de informação existentes num ambiente industrial possuem características de tal forma distintas que não é possível dispor de uma única rede capaz de satisfazer todas

as necessidades de comunicação. Desta forma, a alternativa é dispor de um conjunto de redes que no seu conjunto sejam capazes de satisfazer a totalidade dessas necessidades. Num sistema automatizado as actividades relacionadas com o controlo do processo industrial podem ser estruturadas num modelo hierárquico caracterizado por fluxos de informação verticais entre entidades de níveis hierárquicos adjacentes e por fluxos de informação horizontais entre entidades do mesmo nível hierárquico. Como estas actividades estão intimamente associadas à estrutura de comunicações que lhes serve de suporte, surge de forma natural a adopção de um modelo hierárquico para a arquitectura de comunicações (Figura 2.6) [5].

Figura 2.6 - Relação entre os níveis de controlo e a arquitectura de comunicações

Embora os modelos hierárquicos para a estrutura de controlo possam variar em número de níveis, tipicamente entre o 4 e o 6, ao nível da arquitectura de comunicações é usual identificar três níveis distintos: fábrica, célula e campo. Para cada um destes níveis foram desenvolvidas várias soluções, cada uma possuindo diferentes objectivos, protocolos, capacidades e complexidade:

- Fábrica - Cobrem as necessidades dos níveis superiores. As principais actividades encontradas a este nível são o planeamento da produção, de processos e de materiais e as áreas de engenharia financeira e comercial. O fluxo de informações descendente centra-se essencialmente nas ordens de fabrico e nas informações associadas ao seu escalonamento. No sentido ascendente circulam informações relativas ao estado das ordens de fabrico, à qualidade do processo produtivo e a pedidos de aquisição de materiais e/ou recursos. Este nível é caracterizado por um elevado fluxo de informação horizontal entre e dentro dos vários subsistemas existentes sem requisitos temporais críticos.

- Célula - Cobrem as necessidades dos níveis intermédios. Uma célula agrupa um conjunto de equipamentos que cooperam para a execução de uma determinada tarefa. As principais actividades encontradas a este nível são o escalonamento, o sequenciamento e a execução de tarefas. Outras actividades também executadas têm a ver com a compilação da informação relativa à qualidade da produção e ao desempenho dos equipamentos que constituem a célula. A informação que circula do nível célula para os níveis descendentes inclui ordens de execução de operações ou programas de controlo, no caso de equipamentos programáveis. Em sentido ascendente a informação disponibilizada diz respeito à evolução das operações executadas e aos resultados dessas mesmas operações. Este nível é caracterizado por fluxos de informação de volume intermédio e com requisitos temporais exigentes, que em muitos casos podem ser críticos.
- Campo - Cobrem as necessidades dos níveis mais baixos. As principais actividades encontradas a este nível estão relacionadas com o controlo directo do processo industrial, nomeadamente a execução de algoritmos de controlo, por equipamentos que actuam fisicamente sobre os materiais ou produtos a operar. A *interface* com o processo é realizada por intermédio de sensores e actuadores, muitos deles dotados de capacidades de processamento complexas (*smart sensors*). Este nível é caracterizado por fluxos de informação de pequeno volume e com requisitos temporais críticos.

2.5 Redes de Campo

As redes de campo foram inicialmente desenvolvidas com o objectivo de satisfazer os requisitos de comunicação dos níveis mais baixos das arquitecturas de controlo industriais. Entre estes destacam-se, pela sua importância, os seguintes [14], [15]:

- Capacidade de transferir pequenos volumes de informação de forma eficiente;
- suportar tráfego periódico (por exemplo amostragem de dados) e aperiódico (por exemplo eventos) com tempos de resposta majorados. Existem assim requisitos de tempo real associados às comunicações;
- capacidade de operar em ambientes industriais típicos, sujeitos a interferências electromagnéticas, vibrações, corrosão, poeiras, humidade, etc;
- garantir um nível adequado de confiança no funcionamento, nomeadamente no que diz respeito à fiabilidade, disponibilidade e segurança e
- baixo custo de aquisição, instalação, operação e manutenção.

De forma a satisfazer estes requisitos foi adoptada uma *stack* de comunicação organizada de acordo com o modelo OSI, mas compactada em 3 níveis: físico, ligação de dados e aplicação. O nível de aplicação incorpora algumas funcionalidades definidas nos restantes níveis não utilizados neste modelo.

Para cada um dos níveis podem ser definidos múltiplos serviços e protocolos de comunicação com características muito diversas. A escolha destes elementos resulta essencialmente dos objectivos originais definidos pelos fabricantes das redes de campo, que de uma forma sucinta podem ser expressos segundo duas perspectivas [15]:

- A rede de campo é considerada apenas como uma forma de simplificar as ligações físicas entre os vários dispositivos ou
- a rede de campo é considerada a coluna vertebral (*backbone*) de um sistema distribuído e de tempo-real.

A diferença entre estas duas perspectivas foi uma das razões que levaram à proliferação de soluções para as redes de campo. Outras razões estão relacionadas com a ausência de um *standard* internacional único e genérico.

2.5.1 Standardização das Redes de Campo

Já no início dos anos 70 foram instaladas e utilizadas as primeiras redes de campo. No entanto, o trabalho de standardização só teve início em meados dos anos 80. A ideia básica de um *standard* é estabelecer uma especificação de uma forma muito rígida e formal, excluindo a possibilidade de pequenas alterações. Isto dá uma certa noção de confiabilidade e estabilidade da especificação, que por sua vez assegura a confiança dos utilizadores e consequentemente uma boa posição no mercado. Além disso, em muitos países os *standard*s têm uma posição *legally binding*, o que significa que quando um *standard* pode ser aplicado é obrigatório aplicá-lo. Isto implica que um sistema standardizado ganha uma posição competitiva em relação aos rivais não standardizados. Não é então de admirar que fosse iniciada uma corrida para a standardização.

A standardização internacional das redes de campo foi sempre difícil. Teve o seu início em 1985 e, depois de uns anos entusiásticos de desenvolvimento, a procura de um único *standard* foi ficando enredada numa rede de políticas de companhias e de interesses de *marketing* [7].

Na segunda parte dos anos 80, no início dos trabalhos da comissão técnica TC 65C do IEC (International Electrotechnical Commission) o desenvolvimento dos sistemas

fieldbus foi basicamente um projecto europeu, levado a cabo, não só por investigadores com um *background* académico, mas também por muitos proprietários. Os resultados mais promissores foram o francês FIP e o alemão PROFIBUS. Ambos foram standardizados a nível nacional e posteriormente propostos ao IEC para standardização internacional. No entanto, as abordagens dos dois sistemas eram completamente diferentes. O PROFIBUS baseava-se no controlo distribuído e a sua forma original suportava uma comunicação vertical orientada ao objecto, de acordo com o modelo cliente-servidor, no espírito da especificação MAP/MMS. Por outro lado, o FIP foi desenvolvido segundo um esquema de controlo centralizado mas capaz de suportar comunicação em tempo real, de acordo com o novo modelo para comunicação horizontal produtor-consumidor ou *publisher-subscriver*.

Como eram muito diferentes, os dois sistemas satisfaziam os requisitos de áreas de aplicação diferentes. Evidentemente, um *fieldbus* universal tinha de combinar os benefícios dos dois, pelo que um grupo de peritos apresentou uma nova proposta, o WorldFIP, que é uma extensão do FIP ao qual foi acrescentada a funcionalidade do modelo cliente-servidor. Por outro lado, o ISP (Interoperable System Project) tentou demonstrar que o PROFIBUS poderia ser melhorado com a introdução do modelo de comunicação *publisher-subscriber*. No entanto o ISP foi abandonado em 1994 por razões estratégicas [7].

Ao mesmo tempo, o papel de líder nos trabalhos de standardização ao nível do IEC foi sendo tomado, não pelos europeus, mas pelo comité SP50 do ISA (International Society of Automation), que foi muito mais eficiente no fim dos anos 80 e teve uma influência importante na estrutura de camadas do *standard* actual. No entanto, até meados dos anos 90 o comité do IEC não tinha produzido nenhum resultado substancial durante mais de 8 anos. A única excepção foi a definição da camada física, que foi adoptada como um *standard* IEC 61158-2 em 1993.

Em 1995, depois de longos anos de disputas entre investigadores alemães e franceses, com vista a combinar as abordagens FIP e PROFIBUS, várias companhias, basicamente americanas, decidiram não continuar a testemunhar as infindáveis discussões. Com o fim do projecto ISP, iniciaram a definição de uma nova rede de campo optimizada para a indústria de processos: o FF (Fieldbus Foundation). Este trabalho foi feito à parte dos comités IEC, dentro do ISA, e por algum tempo o trabalho no IEC pareceu posto de parte.

A 15 de junho de 1999 o comité de acção do IEC decidiu tomar um novo rumo e um mês depois, a 16 de Junho, os representantes das principais partes interessadas na

standardização *fieldbus* (Fieldbus Foundation, Fisher Rosemount, ControlNet International, Rockwell Automation, PROFIBUS User Organization e Siemens) assinaram um "Memorando de Entendimento", com o objectivo de pôr um ponto final na disputa dos *standards fieldbus*.

Este processo culminou em 2003 com a adopção de uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 (Digital Data Communications for Measurement and Control - Fieldbus for use in Industrial Control Systems) e o IEC 61784 (Digital Data Communications for Measurement and Control - Profile Sets for Continuous and Discrete Manufacturing Relative to Fieldbus Use in Industrial Control Systems), sendo ambos constituídos por um conjunto de perfis de comunicação, aos quais acabaram por corresponder as soluções comerciais mais importantes existentes à data da sua publicação (Tabela 2.1) [7].

Tabela 2.1 - Perfis e protocolos de acordo com o IEC 61784 e o IEC 61158

IEC 61784 Perfil	IEC 61158 Protocolos-camadas			Standard CENELEC	Nome comercial
	Física	Ligação de dados	Aplicação		
CPF-1/1	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H1)
CPF-1/2	Ethernet	TCP/UDP/IP	Tipo 5	-	Foundation Fieldbus (HSE)
CPF-1/3	Tipo 1	Tipo 1	Tipo 9	EN-50170-A1	Foundation Fieldbus (H2)
CPF-2/1	Tipo 2	Tipo 2	Tipo 2	EN-50170-A3	ControlNet
CPF-2/2	Ethernet	TCP/UDP/IP	Tipo 2	-	Ethernet/IP
CPF-3/1	Tipo 3	Tipo 3	Tipo 3	EN-50254-3	PROFIBUS-DP
CPF-3/2	Tipo 1	Tipo 3	Tipo 3	EN-50170-A2	PROFIBUS-PA
CPF-3/3	Ethernet	TCP/UDP/IP	Tipo 10	-	PROFINET
CPF-4/1	Tipo 3	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-485
CPF-4/1	Tipo 1	Tipo 4	Tipo 4	EN-50170-1	P-Net RS-232
CPF-5/1	Ethernet	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS)
CPF-5/2	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS,MCS, subMMS)
CPF-5/3	Tipo 1	Tipo 7	Tipo 7	EN-50170-3	WorldFIP (MPS)
CPF-6/1	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS
CPF-6/2	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS TCP/IP
CPF-6/3	Tipo 8	Tipo 8	Tipo 8	EN-50170-2	INTERBUS Subset
CPF-7/1	Tipo 1	Tipo 6	-	-	Swiftnet transport
CPF-7/2	Tipo 1	Tipo 6	Tipo 6	-	Swiftnet full stack

Como se pode verificar pela tabela, sistemas *fieldbus* simples, como o CAN e o AS-*Interface*, não foram incluídos nesta norma. Estes estão incluídos num *standard* específico para este tipo de sistemas, o IEC 62026 (Low-voltage switchgear and controlgear - Controller-Device Interfaces), publicado em Junho de 2007.

À medida que o processo de standardização foi estabilizando, o desenvolvimento focou-se na definição de uma quarta camada, denominada camada de utilizador. O seu objectivo é disponibilizar ao utilizador uma abordagem integrada no desenvolvimento das aplicações, nomeadamente através da definição de blocos funcionais, linguagens de descrição dos dispositivos, interoperabilidade e métricas da qualidade de serviço.

Quanto ao seu posicionamento em relação aos níveis de controlo das aplicações industriais, as redes de campo sofreram uma evolução, passando também a ser utilizadas presentemente como redes de célula. A própria terminologia tem evoluído, através da definição de um conjunto de subcategorias para as redes de campo (Figura 2.7) [5]. Neste sentido, o termo original *fieldbus* tem sido utilizado para designar as redes de campo que estão mais próximas do conceito de rede de célula (ex. PROFIBUS-DP, WorldFIP) e o termo *sensorbus* para designar as redes mais básicas e mais próximas do conceito original de rede de campo (ex. AS-Interface, INTERBUS-S), enquanto o termo *devicebus* é utilizado para designar as que estão num plano de actuação intermédio (ex. DeviceNet, FF-H1). Contudo, e por uma questão de simplificação de linguagem, utiliza-se nesta dissertação apenas os termos rede de campo ou *fieldbus* para representar todas as subcategorias acima definidas.

Figura 2.7 - Categorias das redes de campo

2.6 Ethernet em Tempo Real

Ao mesmo tempo que decorria a standardização *fieldbus*, no mundo administrativo eram implementadas redes baseadas na Ethernet e no TCP/IP. Os custos associados a estas

infra-estruturas têm vindo continuamente a baixar e tornou-se possível ligar quase tudo, em qualquer lado do mundo, com a ajuda da tecnologia da Internet. No entanto, no campo da automação, ainda eram utilizados *fieldbuses* dedicados, a única barreira para aceder a componentes no chão de fábrica via Internet.

Depois de mais de 1 década de experiência com aplicações de *fieldbuses* a indústria começou a desenvolver e a adoptar soluções RTE. Os *standard*s propostos pelo IEC tentam traçar uma linha de orientação e critérios de selecção baseados em indicadores reconhecidos.

A adopção da tecnologia Ethernet na comunicação industrial pressupõe capacidades Internet, como por exemplo *interfaces* com o utilizador remotos, via Web. No entanto, é uma solução inaceitável se a adopção da tecnologia Ethernet causa perda de características necessárias no chão de fábrica, tais como [18]:

- Comunicação determinística;
- acções sincronizadas entre componentes e
- troca de pequenos pacotes de dados eficiente e frequente.

Um requisito implícito e essencial é a capacidade de comunicação Ethernet no nível de escritório ser totalmente absorvida, de modo que o *software* de comunicação envolvido possa ser utilizado. Isto resulta nos seguintes requisitos:

- Suporte de migração da Ethernet do nível do escritório para RTE e
- uso de componentes *standard* (*bridges*, controladores Ethernet e *stack*s de protocolo).

Para se obter a necessária alta qualidade de transmissão de dados, com *jitter* limitado e com perturbações devidas ao tráfego de dados TCP/IP limitadas é necessário desenvolver novos componentes de rede.

Resumindo, a RTE é uma especificação *fieldbus* que utiliza a Ethernet nos dois níveis mais baixos.

2.6.1 Standardização RTE

O *standard* Ethernet não atinge os requisitos do RTE. Existem diferentes propostas na comunidade de investigação para a modificação da tecnologia Ethernet. O mercado também adoptou soluções técnicas adicionais. A seguir são apresentadas as soluções RTE propostas para standardização.

As *interfaces* de comunicação estão estruturadas em diferentes níveis. Na figura 2.8 estão representadas as estruturas possíveis de um protocolo de comunicação RTE [18]. Comum a todas as redes Ethernet é a infraestrutura de cablagem universal.

As aplicações *non real time* utilizam os protocolos Ethernet, tal como definido no ISO 8802-3, e o protocolo TCP/UDP/IP. Utilizam ainda protocolos típicos da Internet, tal como o HTTP ou o FTP.

Figura 2.8 - Estruturas possíveis de uma RTE

Para uma solução RTE existem três diferentes abordagens:

- Na primeira mantêm-se os protocolos TCP/UDP/IP e a modificação que garante o tempo real é feita no nível mais alto. É a solução *on top of* TCP/IP.
- Na segunda não são utilizados os protocolos TCP/UDP/IP e a funcionalidade Ethernet é acedida directamente. É a solução *on top of Ethernet*.
- Na terceira abordagem o mecanismo Ethernet e a própria infraestrutura são modificados de forma a obter uma *performance* em tempo real. É a *Modified Ethernet*.

Na secção seguinte são apresentados os protocolos RTE que existem no mercado.

2.6.2 Protocolos RTE

O IEC 61784-2 (Industrial Communication Networks - Profiles – Part 2: Additional Fieldbus Profiles for Real time Networks based on ISO/IEC 8802-3) é o documento *standard* que especifica pelo menos dez diferentes soluções técnicas para RTE, sendo muitas delas incompatíveis [18] (Tabela 2.2). Alguns dos protocolos propostos apenas

estão definidos, não existindo ainda produtos no mercado. No caso de outros protocolos já existem produtos e aplicações.

Tabela 2.2 - Perfis RTE definidos no IEC 61784

Perfil IEC 61784	**Nomes comerciais**	***Ethertypes***
CPF-2	ControlNet (Ethernet/IP)	(0x0800 IP)
CPF-3	PROFIBUS/PROFINET	0x8892
CPF-4	P-NET	(0x0800 IP)
CPF-10	Vnet/IP	(0x0800 IP)
CPF-11	*TCnet* (Time Critical control network)	0x888B
CPF-12	EtherCAT	0x88A4
CPF-13	EPL (Ethernet PowerLink)	0x88AB
CPF-14	EPA (Ethernet for Plant Automation)	0x88BC
CPF-15	MODBUS – RTPS (Real Time Publisher Subscriber).	(0x0800 IP)
CPF-16	SERCOS (SErial Real time COmmunication System Interface)	0x88CD

Protocolos *on top of* TCP/IP

Algumas soluções RTE utilizam a *stack* do protocolo TCP/UDP/IP sem modificações. Com esta *stack* é possível comunicar de uma forma transparente para além dos limites da rede de campo.

É então possível implementar redes de campo que comuniquem com todos os pontos do mundo, da mesma forma que a tecnologia Internet. No entanto, o manuseamento desta *stack* de protocolo de comunicação requer recursos razoáveis, quer ao nível do processamento, quer ao nível da memória e introduz atrasos não determinísticos na comunicação.

A seguir são apresentadas algumas soluções disponíveis no mercado.

Modbus/TCP

Foi definido pela Schneider Electric e é mantido pela Modbus-IDA. Utiliza o já conhecido Modbus (o *standard* industrial “de facto” desde 1979) sobre uma rede TCP/IP, através da porta 502.

Esta é provavelmente uma das soluções Ethernet mais utilizadas em aplicações industriais e satisfaz os requisitos da classe mais baixa de aplicações, o controlo humano.

É um protocolo muito simples, do tipo *request/reply* (envia uma trama de *request* e recebe uma trama de *reply*). Em adição ao histórico Modbus, este protocolo tem definidas extensões *real time* que utilizam o RTPS. O RTPS prevê dois modelos de comunicação: o

publisher-subscriber, que transfere dados do *publisher* para o *subscriber*, e o CST (Composite State Protocol), que transfere informação de estado de um escritor para um leitor.

Ethernet/IP

Este protocolo foi definido pela Rockwell e é mantido pela ODVA (Open DeviceNet Vendor Association) e pela ControlNet International. Utiliza o CIP, que é comum nas redes Ethernet/IP, ControlNet e DeviceNet.

Este protocolo está incluído no *standard* IEC 61784-1 como CP 2/2 (tipo 2 no IEC 61158) e fornece comunicação *real time* baseada no ISO/IEC 8802-3.

Na Ethernet *full-duplex* não existe a possibilidade de atrasos devidos a colisões. No entanto, as tramas Ethernet podem sofrer atrasos no próprio dispositivo de *switch*, caso a porta de saída esteja ocupada na transmissão de outra trama. Isto pode levar a atrasos não determinísticos, que não são aconselháveis em aplicações em tempo real. Para evitar estes atrasos está definido um mecanismo de prioridades no IEEE 802.3, que permite a atribuição de níveis de prioridade (0 a 7) a tramas Ethernet.

P-NET

O P-NET sobre a especificação IP foi proposto pelo comité nacional dinamarquês e o seu uso destina-se ao ambiente IP. Neste protocolo a comunicação em tempo real P-NET é embebida em pacotes UDP/IP, que tanto podem circular em redes IP como em redes *non* IP.

Uma trama P-NET inclui uma tabela P-Net *route*, que por sua vez é constituída por dois elementos: os endereços da fonte e do destino da própria trama. No caso mais simples de uma rede de campo, estes são os endereços de dois nós da própria rede. Para permitir a comunicação entre dispositivos da rede de campo e dispositivos de uma rede IP os endereços da tabela P-Net *route* terão de ser endereços IP.

De facto, este protocolo apenas especifica a forma como são integradas redes P-NET e redes UDP/IP e não prevê nenhuma medida que assegure um comportamento em tempo real na rede Ethernet.

Vnet/IP

Este protocolo foi desenvolvido pela Yokogama.

Utiliza o TCP/IP para a integração de protocolos Internet, como o HTTP, e de extensões de protocolos *real time*, o RTP (Real Time and reliable datagram Protocol).

Este não é de facto um protocolo RTE, apenas utiliza o protocolo UDP/IP para o transporte do protocolo RTP. Não são tomadas nenhumas medidas especiais que garantam o comportamento determinístico de um protocolo *real time*.

Protocolos *on top of* Ethernet

Estes protocolos RTE não alteram o *hardware* de comunicação Ethernet, mas especificam um tipo de protocolo especial na trama Ethernet, o *Ethertype* (tabela 2.2). Por exemplo, o tipo *standard* para o protocolo IP é *Ethertype*=0X0800. Estes protocolos RTE utilizam, além da *stack* de protocolo IP *standard*, a sua própria *stack* de protocolo identificada com o seu próprio tipo. A tabela 2.2 lista os diferentes valores assignados para as várias soluções.

EPL

Foi definido por Bernecker & Rainer e é mantido pelo grupo de standardização EPL.

Baseia-se num sistema de escalonamento *master-slave* num segmento Ethernet partilhado, o SCNM (Slot Communication Network Management). O *master* é o MN (Managing Node), assegura o acesso em tempo real aos dados cíclicos e apenas permite a comunicação de tramas TCP/IP (*non real time*) em *slots* de tempo reservadas para este tipo de dados. Todos os outros nós são os CNs (Controlled Nodes) e apenas podem enviar dados a pedido do MN.

O ciclo de comunicação de um sistema EPL é composto por quatro períodos: *Start*, *Isochronous*, *Asynchronous* e *Idle* (Figura 2.9) [18]. No período *Start* o MN envia uma trama *multicast* SoC (Start of Cycle), que indica o início do ciclo. No período *Isochronous* o MN envia uma trama *unicast* PReq (Poll Request) para cada um dos CNs e o CN acedido envia uma trama *multicast* PRes (Poll Response). No início do período *Asynchronous* o MN envia uma trama SoA (Start of Asynchronous) e o acesso ao meio é permitido tanto ao MN como a qualquer CN, mas apenas pode ser enviada uma trama ASnd (ASynchronous data). O protocolo tipicamente usado neste período é o UDP/IP. Desta forma a transmissão de dados assíncronos nunca interfere com a transmissão de dados síncronos, o que garante um *timing* preciso na comunicação.

Figura 2.9 - Ciclo de comunicação do EPL

TCnet

É uma proposta da Toshiba. Tal como no EPL, a *interface* TCnet está entre a camada física e a camada de ligação de dados. O acesso MAC (Medium Access Control) típico da Ethernet, o CSMA/CD, é modificado.

O período de transmissão de alta velocidade é composto por um serviço de transmissão de dados cíclico em tempo real (no TCnet utiliza-se a expressão *time critical*) e por um serviço de transmissão assíncrona (no TCnet é denominada como *sporadic*) (Figura 2.10) [18].

Cada período de transmissão de alta velocidade é iniciado com o *broadcast* de uma trama SYN para todos os nós da rede. Depois de receber a trama SYN, o nó 1 inicia a transmissão das suas tramas de dados (DT). Quando termina faz o *broadcast* de uma trama CMP, que indica o fim da sua transmissão. Esta é recebida pelo nó 2, que inicia a transmissão das suas tramas de dados, repetindo-se o processo até ao último nó.

Figura 2.10 - Ciclo de comunicação do TCnet

EPA

O protocolo EPA é uma proposta chinesa.

Este protocolo permite uma comunicação determinística baseada num mecanismo de divisão de tempo dentro da camada MAC. O *macrocycle* (T) é o tempo total para completar um procedimento de transmissão de dados. Esse tempo é dividido em duas fases: a fase para transmissão de mensagens periódicas (Tp) e a fase para transmissão de mensagens aperiódicas (Tn) (Figura 2.11) [18].

A última parte de cada mensagem periódica é um anúncio de mensagem não periódica, que indica se o dispositivo que enviou a mensagem periódica tem ou não uma mensagem não periódica para transmitir. Se tiver, o dispositivo só a poderá enviar na fase Tn.

Figura 2.11 - Ciclo de comunicação do EPA

PROFINET CBA

Foi definido por um conjunto de vários fabricantes, incluindo a Siemens, e é mantido pela PROFIBUS Internacional.

A primeira versão foi baseada no CBA (Component Based Automation) e está incluída no IEC 61784-1 (tipo 10 no IEC 61158).

Para a transmissão de dados sem requisitos de tempo real é utilizada a *stack* TCP/IP e protocolos como o RPC (Remote Procedure Call) e o DCOM (Distributed Component Object Model). Quando é necessária comunicação em tempo real (para ciclos de tempo abaixo dos 100 ms) não é utilizada a *stack* TCP/IP, sendo preferido o protocolo em tempo

real, que é baseado no *Ethertype* 0x8892 e no mecanismo de atribuição de prioridade à trama.

Modified Ethernet

A topologia da cablagem típica da Ethernet é a topologia em estrela: todos os componentes estão ligados a um dispositivo central de *switch*.

Nas aplicações da área da automação, com a introdução do *fieldbus* a topologia em estrela foi substituída por topologias em barramento ou em anel para reduzir os custos na cablagem.

As soluções RTE devem estar preparadas, tanto para as topologias utilizadas no chão de fábrica, como para a topologia da *swicthed Ethernet*. Para isso existem duas soluções: ou a infraestrutura da rede de campo tem um *switch* para cada dispositivo, ou a funcionalidade de *switch* é integrada nos próprios dispositivos da rede de campo.

SERCOS

O SERCOS III é uma extensão RTE do SERCOS, definido pelo *standard* IEC 61491 (Electrical Equipment of Industrial Machines – Serial Data for Real-Time Communication for Controls and Drives), o seu processo de standardização teve início em 2005 e culminou em 2007 com a aprovação do *standard* IEC 61784-2/61158.

No sistema SERCOS existe uma estação *master* e estações *slave*s, cujo número pode variar entre 1 e 254. Todas as estações têm duas portas Ethernet. A topologia da rede pode ser *daisy-chain* ou em anel. Não são permitidos *switches* entre estações e, apenas no caso da topologia *daisy chain*, a porta Ethernet livre do último *slave* pode ser ligada a um *switch*, se for requerida comunicação entre dispositivos via TCP/IP ou UDP/UDP.

No sistema SERCOS III o ciclo de comunicação está dividido em dois períodos, denominados de canais de comunicação: o primeiro é o canal *real time* e o segundo, com menor duração, é o canal *non real time* (Figura 2.12) [18].

O ciclo de comunicação é iniciado pelo *master*, que envia a t*odos os slaves* dois tipos de telegramas *real time*: até 4 MDTs (Master Data Telegrams) e até 4 ATs (Answer Telegrams). Os MDTs contêm informação para sincronização, informação de controlo, dados de serviço do canal e valores de comando. Os ATs são transmitidos pelo *master* como uma trama vazia, mas com campos pré definidos, sendo cada um desses campos destinado a um determinado *slave*. Se um *slave* pretende enviar informação coloca-a no

seu campo e envia o telegrama AT. Quando termina o canal *real time* é iniciado o canal *non real time*, durante o qual podem ser enviados telegramas *non real time*.

Figura 2.12 - Ciclo de comunicação do SERCOS III

ETHERCAT

Este protocolo foi definido pela Beckoff e é mantido pelo grupo de tecnologia Ethercat (ETG). Utiliza as tramas Ethernet e uma topologia em anel especial.

Utiliza um mecanismo de acesso ao meio do tipo *master-slave*, no qual o nó *master* (tipicamente o sistema de controlo) envia tramas *Ethernet standards* ISO/IEC 8802-3 para os nós *slaves*, que por sua vez recebem e enviam dados através dessas tramas.

PROFINET IO

Este protocolo foi definido por vários fabricantes, sendo o mais importante a Siemens, e é mantido pela PROFIBUS Internacional.

Depois da definição PROFINET CBA, o passo seguinte foi a definição de um modelo de aplicação para o PROFINET IO baseado no PROFIBUS DP (tipo 3 do IEC 61158).

Num sistema deste tipo existem três tipos de dispositivos: os controladores IO, os dispositivos IO e o supervisor IO. Os controladores IO controlam os dispositivos IO com comunicação de dados cíclica através de um *buffer*. O supervisor IO gere o funcionamento dos componentes IO e dos controladores IO do sistema.

O ciclo de troca de dados entre os componentes de um sistema PROFINET IO é dividido nas seguintes fases de comunicação: IRT (Isochronous Real Time), RT (Real Time) e NRT (Non Real Time) (Figura 2.13) [18].

Na fase *Isochronous* a comunicação é escalonada no tempo: em cada tempo de offset a trama IRT é enviada de uma porta para outra sem interpretação do endereço por parte do switch. Nas fases seguintes os *switches* comportam-se como *switches standard* Ethernet, passando a comunicação a ser baseada no endereço. Primeiro são transmitidas as tramas RT durante a fase RT e quando esta termina é iniciada a fase NRT, durante a qual são transmitidas as tramas NRT.

Figura 2.13 - Ciclo de comunicação do PROFINET IO

2.7 Conclusão

Neste capítulo foram abordadas as redes de comunicação industriais, tendo sido feita uma análise aos principais protocolos actualmente utilizados.

Pode-se questionar sobre a necessidade do desenvolvimento de tantos protocolos. No entanto, tal facto é justificado, por um lado, pela pressão dos vários grupos económicos e, por outro, pela complexidade e variedade das possíveis áreas de aplicação.

Em relação a este segundo aspecto, é de facto difícil de conceber que uma única norma consiga abranger todas as áreas de aplicação e, nas várias tentativas feitas, provou-se que tal norma se tornava demasiado complexa, tendo um custo de implementação demasiado alto.

Quanto ao primeiro ponto, é evidente que as empresas fabricantes de sistemas e equipamento não tinham, e não têm, interesse em divulgar os protocolos de comunicação, para proteger os investimentos feitos em termos de I&D (Investigação e Desenvolvimento).

No entanto, depois de muitos anos de esforços foi adoptada uma solução de compromisso da qual resultaram dois *standard*s internacionais: o IEC 61158 e o IEC 61784, que englobam as soluções comerciais mais importantes, incluindo soluções RTE.

Compete ao utilizador final e ao mercado decidir quais das soluções propostas preenchem os requisitos das aplicações em automação.

3 Redes de Comunicações Sem Fios

3.1 Introdução

O emergente paradigma dos sistemas ubíquos leva à necessidade de utilização de sistemas de comunicação sem fios, uma vez que seria insustentável e impraticável o desenvolvimento de sistemas em grande escala com cablagem associada.

O grande benefício das redes sem fios é o facto de o custo associado ao desenvolvimento, manutenção e expansão deste tipo de redes ser extremamente baixo, comparativamente com as soluções tradicionais. Outros benefícios que esta tecnologia proporciona são: a facilidade de instalação de redes temporárias, a eliminação do custo associado a reparações de cabos danificados, bem como a possibilidade de alterações numa rede sem necessidade de reorganização. Estas vantagens tornam as redes sem fios de área local uma solução extremamente interessante para implementar instrumentação em sistemas de automação industrial.

Uma das primeiras decisões no desenvolvimento de uma aplicação deste tipo é a escolha da tecnologia de comunicações a utilizar na transmissão de informação. A tecnologia WLAN (Wireless Local Area Network) mais implementada no mercado é a Wi-Fi. A Wi-Fi opera na banda ISM (Industrial, Scientific and Industrial) não licenciada dos 2.4 GHz (2400 a 2483.5 MHz), com taxas de transmissão de dados próximas dos 11 ou dos 54 Mbps, dependendo da técnica de modulação utilizada. Se o raio de acção desejado for inferior a 10 metros devem ainda ser consideradas as WPAN (Wireless Personal Area Network), como a tecnologia Bluetooth ou a Zigbee.

O objectivo principal deste capítulo é efectuar uma análise às tecnologias de comunicação sem fios existentes no mercado. Esta análise tem como finalidade a escolha de uma tecnologia de comunicação sem fios para implementar o sistema de instrumentação proposto. Assim, na secção 3.2 é feita uma abordagem à tecnologia utilizada por este tipo de redes: a rádio frequência. A seguir, na secção 3.3 são analisados os *standards* da família

IEEE 802 ao nível das redes WLAN e WPAN. Por fim, na secção 3.4 são apresentadas as soluções comerciais com maior implementação no mercado.

3.2 Rádio Frequência

A tecnologia rádio utilizada na comunicação em redes sem fios é baseada na tecnologia *Spread Spectrum*.

A tecnologia *Spread Spectrum* foi desenvolvida durante a 2ª Guerra Mundial para dotar as comunicações militares de grande segurança. Trata-se de uma técnica que espalha o sinal ao longo de um determinado número de frequências, dificultando desta forma a sua intercepção. Algumas das características que tornam esta técnica ideal para a comunicação sem fios são: a possibilidade de coexistência entre sistemas rádio sem perturbação das suas actividades e ainda a possibilidade de operação na banda ISM.

Existem basicamente dois tipos de modulações *Spread Spectrum*: a FHSS (Frequency Hopping Spread Spectrum) e a DSSS (Direct Sequence Spread Spectrum). Em seguida são explicadas estas duas técnicas de modulação, sendo ainda abordada a técnica OFDM (Orthogonal Frequency Division Multiplexing), que é utilizada como técnica de modulação na variante IEEE 802.11a.

A técnica de modulação FHSS foi concebida originalmente como um meio de esconder uma transmissão a pessoas indesejadas. Actualmente é utilizada para outros fins, tais como a redução do nível de interferência. A *Frequency Hopping*, ou salto na frequência, funciona da seguinte maneira: o sinal é transmitido numa frequência por um curto período de tempo e em seguida salta para uma nova frequência. Ao longo de um determinado período de tempo a potência do sinal é espalhada por uma banda de frequências (Figura 3.1) [20]. A sequência de saltos na frequência é predeterminada.
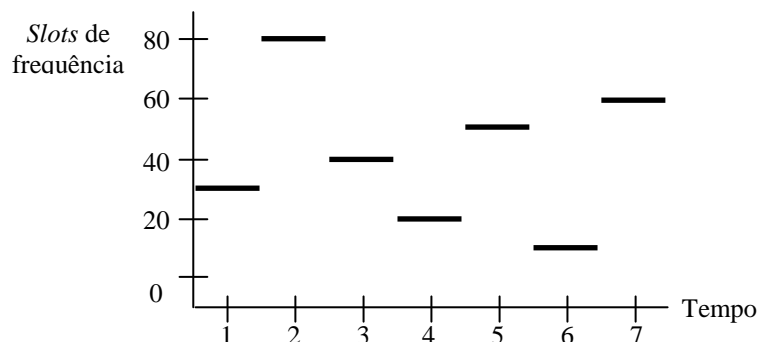
Figura 3.1 - Técnica de modulação FHSS

A DSSS é uma técnica mais complexa que a FHSS. Consiste na distribuição da potência do sinal a transmitir ao longo de uma largura de banda, espalhando a portadora por essa largura de banda. Este procedimento é efectuado modulando directamente a portadora com um código, o *chip-code* (Figura 3.2) [20].
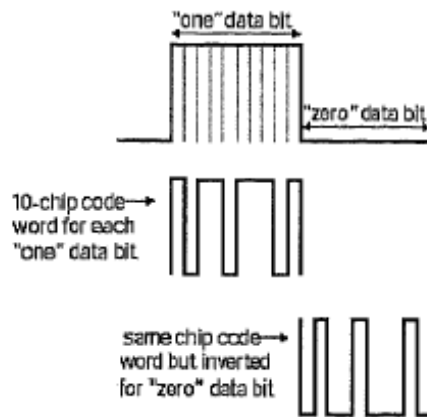
Figura 3.2 - Técnica de modulação FHSS

A sequência de espalhamento é produzida a partir da modulação do fluxo de dados com o *chip-code*, resultando num sinal com uma largura de banda muito maior. Por exemplo, na rede IEEE 802.11 cada *bit* de dados é combinado logicamente com o código de 11 *bits* de Barker. Como a taxa da sequência espalhada é muito maior do que a taxa de dados, a largura de banda é espalhada por uma área muito superior àquela que seria utilizada se o fluxo de dados fosse apenas modulado com a portadora. Como resultado, a potência do sinal é espalhada por uma banda muito maior e com uma aparência de ruído de baixa potência para os outros dispositivos.

Uma técnica de modulação mais recente e utilizada em alguns tipos de comunicações sem fios é a técnica OFDM. Esta é uma técnica baseada em modulação FDM (Frequency Division Multiplexing). Efectua o processo de espalhamento do sinal dividindo-o em pequenas fracções e transmitindo cada uma destas fracções numa frequência diferente. Assim é conseguida uma transmissão rápida através de múltiplas transmissões lentas, utilizando diferentes frequências.

Em seguida serão analisadas várias tecnologias de transmissão sem fios para a comunicação nas LANs e nas PANs. Estas tecnologias vão fazer uso das técnicas de modulação que foram descritas nesta secção.

3.3 *Standard*s sem fios

3.3.1 *Standard*s da família IEEE 802.11

O *standard* IEEE 802.11 foi publicado em 1997 e actualmente inclui especificações que definem as camadas mais baixas do modelo OSI, a camada física e a camada MAC para WLANs. Recorrendo a tecnologia de rádio frequência, o standard IEEE 802.11 transmite e recebe dados, utilizando o ar como canal de comunicação, minimizando assim a necessidade de ligações físicas.

Nas secções seguintes é realizada uma breve análise aos vários *standards* e grupos de trabalho que fazem parte da família do IEEE 802.11.

IEEE 802.11a

O IEEE 802.11a é *standard* desde 1999 e define uma das várias camadas físicas do protocolo IEEE 802.11, na banda ISM dos 5 GHz. As principais características deste *standard* são: velocidades de transferência elevadas (54 Mbps), maior número de canais (12 canais) e distâncias de transmissão até 100 metros. A maior taxa de entrega de dados e o maior número de canais fornece uma melhor protecção contra a interferência dos APs (Access Points) vizinhos.

Nos EUA este *standard* pode operar na banda dos 5,150 a 5,350 GHz e na banda dos 5,725 a 5,825 GHz. Noutros países estas bandas encontram-se alocadas a outras tecnologias e fins, como é o caso da Europa, onde esta banda não está disponível, estando disponível uma faixa entre os 5,470 e os 5,725 GHz.

O IEEE 802.11a utiliza a técnica de modulação OFDM. Dos 12 canais definidos neste *standard* 8 são não sobrepostos e têm uma largura de 20 MHz cada. Assim, teoricamente pode transmitir 432 Mbps (8 canais x 54 Mbps). Cada um destes canais está dividido em 52 sub-portadoras de cerca de 300 KHz. Destas sub-portadoras apenas 48 são utilizadas para transportar dados, sendo as restantes usadas para controlo de erros.

Os dispositivos que implementam o IEEE 802.11a suportam velocidades de 6, 12 e 24 Mbps, sendo as velocidades de 9, 18, 36, 48 e 54 Mbps opcionais. No entanto, as taxas de transmissão mais elevadas apenas funcionam em perfeitas condições para distâncias de transmissão curtas.

Para cada uma das sub-portadoras é utilizada a técnica de modulação de sinal PSK (Phase Shift Keying) ou QAM (Quadrature Amplitude Modulation), dependendo da velocidade seleccionada.

A maior desvantagem deste *standard* é o facto de ele não ser compatível com os outros níveis físicos especificados no IEEE 802.11, isto é, um dispositivo equipado com tecnologia IEEE 802.11a não pode comunicar directamente com outro dispositivo IEEE 802.11b ou IEEE 802.11g. As grandes vantagens desta tecnologia são: a taxa de transferência de dados elevada e a localização numa banda de frequências limpa e livre de interferências e bom desempenho a curtas distâncias. A capacidade de rede elevada deve-se ao suporte até 8 APs numa área, uma vez que possui o mesmo número de canais não sobrepostos, comparado com os 3 canais não sobrepostos do IEEE 802.11b e do IEEE 802.11g.

IEEE 802.11b

O IEEE 802.11b é, desde 1999, *standard* para a camada física do IEEE802.11 na banda dos 2.4 GHz e é o mais implementado actualmente no mercado.

Esta banda é actualmente utilizada para a maioria das transmissões não licenciadas, sendo igualmente utilizada pelo IEEE 802.11g. Oferece 83 MHz de espectro para todo o tipo de tráfego, incluindo telefones sem fios, transmissões entre edifícios, microondas e outras tecnologias de comunicações sem fios.

O IEEE 802.11b utiliza um método de transmissão DSSS e pode transmitir a taxas de 5,5 e 11 Mbps, para além dos 1 e 2 Mbps do *standard* inicial. Para proporcionar taxas de transmissão mais elevadas o IEEE 802.11b utiliza a técnica de modulação CCK (Complementary Code Keying).

O IEEE 802.11b divide o espectro em 14 canais, estando apenas disponíveis 11, tendo cada canal uma largura de banda de 25 MHz. Assim, apenas podem ser usados simultaneamente 3 canais, permitindo uma taxa de transferência acumulada de 33 Mbps contra os 432 Mbps permitidos pelo IEEE 802.11a. Suporta até 32 utilizadores por AP.

Um ponto negativo neste *standard* é a alta interferência, tanto na transmissão como na recepção de sinais, porque funciona na banda ISM dos 2,4 GHz, tal como os telefones móveis, os fornos microondas e os dispositivos Bluetooth. Os aspectos positivos são o baixo preço dos produtos actualmente existentes no mercado, a interoperabilidade entre

todos os fabricantes (certificação Wi-Fi), a compatibilidade entre este *standard* e o IEEE 802.11g, a transmissão a longas distâncias (500 metros em exterior e 100 metros em interiores), o baixo consumo de energia e o facto de existir uma larga base de redes instaladas. O 802.11b é amplamente usado por utilizadores de Internet sem fio.

IEEE 802.11d

O IEEE 802.11d foi publicado em 2001 e tem como objectivo promover a harmonização das WLANs a nível mundial. Permite que os APs possam comunicar através de canais rádio com níveis de potência aceitáveis. Uma vez que o IEEE 802.11 não pode operar legalmente em alguns países, o objectivo da extensão IEEE 802.11d é adicionar especificações e restrições de modo a possibilitar a operação destes *standards* nesses países, especialmente no que diz respeito ao IEEE 802.11a, que comunica na banda dos 5 GHz.

IEEE 802.11e

É *standard* desde 2005 e é um suplemento para a camada MAC, com o objectivo de agregar qualidade de serviço (QoS - Quality of Service) nas redes IEEE 802.11, a aplicações de transmissão de voz e vídeo. Permite a diferenciação do tráfego para que seja possível a sua ordenação. A sua aplicação estende-se aos *standards* IEEE 802.11a, b e g.

Em suma, o IEEE 802.11 permite a transmissão de diferentes classes de tráfego e inclui o recurso TXOP (Transmission Oportunity). O TXOP consiste num intervalo de tempo durante o qual as estações com QoS podem transmitir dados, optimizando assim a utilização da rede.

IEEE 802.11f

É um documento de recomendação de práticas para que os produtos dos diferentes fabricantes sejam interoperantes. Recomenda aos fabricantes a utilização de equipamentos de WLAN que permitam a interoperação entre os APs e define o protocolo IAPP (Inter Access Point Protocol).

IEEE 802.11g

O IEEE 802.11g foi publicado em 2003 e é a terceira extensão à camada física do IEEE 802.11 a ser *standard*. Funciona na banda ISM dos 2,4 GHz e especifica a existência de três canais de rádio não sobrepostos, tal como o IEEE 802.11b. Em relação ao IEEE 802.11a, a cobertura de uma grande área com grande densidade de utilizadores é mais difícil.

A taxa máxima de transferência de dados é de 54 Mbps. Para poder transmitir a velocidades elevadas o IEEE 802.11g utiliza a modulação OFDM. No entanto, para ser compatível com o antecessor IEEE 802.11b, suporta uma modulação CCK. Para manter essa compatibilidade a velocidade de transferência tem que estar reduzida a 11 Mbps. O número excessivo de modulações resulta num *standard* complexo, quando comparado com o IEEE 802.11a. Um dos maiores problemas do IEEE 802.11g, a funcionar em conjunto com o IEEE 802.11b, é a interferência RF com outros dispositivos na banda dos 2,4 GHz. Consegue-se diminuir este problema através da eliminação das fontes de ruído, mas nunca se consegue resolver completamente. A degradação da comunicação com a distância ou a interferência, com consequente perda de comunicação, é um dos maiores problemas que se colocam ao crescimento deste *standard*.

A venda de produtos relacionados com este *standard* já ultrapassou largamente a venda de produtos IEEE 802.11b. O seu sucesso deve-se principalmente à taxa de transmissão elevada. Algumas soluções proprietárias anunciam mesmo taxas de 108 Mbps.

IEEE 802.11h

Este *standard* foi publicado em 2003 e vai ao encontro de algumas regulamentações para a utilização da banda de 5 GHz na Europa. O IEEE 802.11h conta com dois mecanismos que optimizam a transmissão via rádio: a tecnologia TPC (Transmit Power Control), que permite que o rádio ajuste a potência do sinal de acordo com a distância do receptor, e a tecnologia DFS (Dynamic Frequency Selection), que permite a escolha automática de canal, minimizando a interferência noutros sistemas que operem na mesma banda.

IEEE 802.11i

O IEEE 802.11i é *standard* desde 2004 e é uma tentativa do IEEE para diminuir os ataques contra as redes que utilizam o protocolo IEEE 802.11. Este *standard* proporciona uma alternativa ao *WEP (Wired Equivalent Privacy) com novos* procedimentos de encriptação, tendo como objectivo diminuir as fraquezas presentes no WEP. Como as debilidades do WEP são bastante conhecidas, o protocolo IEEE 802.11 criou novos procedimentos tais como: substituir as chaves temporais utilizadas no WEP pelo protocolo TKIP (Temporal Key Integrity Protocol). O protocolo TKIP proporciona troca de informação segura e troca de chaves dinâmicas. Para tal, continua a utilizar o algoritmo de encriptação RC4, o mesmo do WEP, mas com alterações importantes:

Chaves dinâmicas - permite chaves dinâmicas por sessão e por pacote MAC, chave criptográfica usando o endereço MAC do remetente e do destinatário e o campo de dados para se proteger contra ataques. Verifica a integridade da recepção dos dados;

Vector de inicialização de 48-*bit* - diminui a fraqueza da chave de 24-*bit*, se recebido fora de ordem é imediatamente descartado;

Correcção da vulnerabilidade do WEP em que o vector de inicialização é enviado na forma de texto.

O grande benefício deste protocolo é a resolução do problema das chaves estáticas. O uso de um vector de inicialização de 48 *bit* vai aumentar o tempo de vida da chave, eliminando a necessidade de utilização de chaves repetidas durante uma sessão.

Para aumentar o tempo de vida do protocolo IEEE 802.11i o IEEE pretende trocar o algoritmo RC4 pelo método de encriptação AES (Advanced Encryption Protocol), mais robusto do que o anterior. O AES utiliza o algoritmo de Rijndael com chaves de 128, 192 e 256 *bits*, bastante mais robustas que as utilizadas pelo WEP.

IEEE 802.11j

Foi publicado em 2004 e diz respeito às bandas que operam nas faixas de 4,9 GHz e 5 GHz, disponíveis no Japão.

IEEE 802.11k

Possibilita um meio de acesso para os APs transmitirem dados de gestão.

O IEEE 802.11k permite transições transparentes do BSS (Basic Service Set) no ambiente WLAN. Esta norma fornece informações para a escolha do melhor AP disponível que garanta o QoS necessário.

IEEE 802.11n

Tem a largura de banda de 104 Mbps e opera nas faixas de 2,4 GHz e 5 GHz. Promete ser o *standard* sem fios para distribuição de dados de voz e vídeo, pois oferece, através de configurações MIMO **(**Multiple Input, Multiple Output**)**, taxas mais altas de transmissão (até 600 Mbps), maior eficiência na propagação do sinal e ampla compatibilidade com os outros protocolos.

IEEE 802.11p

É utilizado para implementação veicular.

IEEE 802.11r

Especifica o *hand-off* rápido quando um cliente se reassocia após uma deslocação de um AP para outro na mesma rede.

IEEE 802.11s

Especifica o *self-healing/self-configuring* nas redes *Mesh*.

IEEE 802.11t

É um conjunto de normas que provêm de métodos de testes e métricas.

IEEE 802.11u

Promove a interoperabilidade com outras redes sem fios.

IEEE 802.11v

É o *standard* de gestão de redes sem fio para a família IEEE 802.11, mas ainda está em fase inicial de propostas. O *Task Group* v do IEEE 802.11 (TGv), grupo encarregado de definir o *standard* 802.11v, está a trabalhar numa adenda ao *standard* IEEE 802.11 para permitir a configuração de dispositivos clientes ligados a redes IEEE 802.11.

3.3.2 *Standards* da família IEEE 802.15

O IEEE 802.15 é um conjunto de *standards* focados nas redes WPAN. Este conjunto de *standards* define os níveis físico e de ligação de dados do modelo de referência OSI.

As principais características que esta família de *standards* pretende implementar são a comunicação a pequena distância, o baixo consumo de energia e o baixo custo.

O IEEE 802.15 está dividido em vários *standards* para diversos níveis de aplicação dentro das WPAN. Em seguida realiza-se uma pequena descrição sobre cada um dos *standards* do IEEE 802.15.

IEEE 802.15.1

Este *standard* foi publicado em 2005 e não é mais do que a conversão da especificação Bluetooth para um *standard* IEEE. Permite total interoperabilidade com a especificação Bluetooth.

IEEE 802.15.2

O IEEE 802.15.2 foi publicado em 2003. É um documento de recomendação de práticas para a coexistência entre dispositivos WPAN e outros dispositivos sem fios a funcionar dentro da mesma gama de frequências.

IEEE 802.15.3

O IEEE 802.15.3 foi publicado em 2003. É um *standard* para altas velocidades de comunicação (> 20 Mbps) na WPAN, baixo consumo e baixo preço. Tem como objectivo satisfazer a necessidade de aplicações multimédia tais como: vídeo e imagem digital, incluindo QoS.

IEEE 802.15.4

O IEEE 802.15.4 foi publicado em 2006. É um *standard* para baixas velocidades de comunicação (< 200 Kbps) e baixo consumo (bateria com duração de meses ou anos). Este standard é destinado a aplicações que necessitem de baixas taxas de transmissão, tais como redes de sensores e actuadores, brinquedos, controlos remotos e automação de casas.

3.4 Tecnologias sem fios

3.4.1 IEEE 802.11/Wi Fi

É adoptado pela primeira vez em 1997 como *standard* para WLANs e é revisto mais tarde em 1999. Nas secções seguintes é analisada a arquitectura deste protocolo e o modo de funcionamento da rede IEEE 802.11.

Topologia da rede

O protocolo IEEE802.11 é baseado numa topologia celular, em que o sistema é subdividido em várias células. Cada célula, designada por BSS, é controlada por uma estação base, designada por AP. No entanto, uma rede pode ser formada por uma única célula com um único AP, podendo mesmo funcionar sem recurso a AP. A maior parte das instalações é formada por diversas células, onde os APs estão ligados por um tipo de *backbone* designado por DS (Distribution System). Este *backbone* é tipicamente construído com recurso a cablagem (*Ethernet*), mas em alguns casos também pode ser construído com base em tecnologia sem fios.

Toda a WLAN, incluindo as diferentes células e respectivos APs e DSs, é vista como uma única rede para os níveis superiores do modelo OSI e é denominada como ESS (Extended Service Set).

Em seguida apresenta-se uma definição um pouco mais pormenorizada dos componentes de rede que constituem uma WLAN IEEE 802.11.

Estação – é o componente que efectua a ligação ao meio. Suporta serviços de autenticação, não autenticação, privacidade e entrega de dados;

BSS - é uma célula, isto é, um conjunto de estações que comunicam umas com as outras. Quando todas as estações da BSS são estações móveis e não existe qualquer ligação

a uma rede com fio, a BSS é chamada de IBSS (Independent Basic Service Set). Esta é uma rede ponto a ponto, *ad-hoc*, com uma vida curta e com um pequeno número de estações, criada para uma determinada situação em particular. Quando a BSS inclui um AP então é uma BSS estruturada e a rede é do tipo cliente-servidor. Se existe um AP e a estação móvel necessitar de comunicar com outra estação, a comunicação é enviada primeiro para o AP e depois deste para a outra estação móvel. Este procedimento consome o dobro da largura de banda, no entanto, os benefícios proporcionados pelo AP ultrapassam esse custo. Um desses benefícios, por exemplo, é o armazenamento do tráfego de uma estação enquanto esta está a operar no estado de baixo consumo de energia.

ESS - conjunto de BSSs estruturadas onde os pontos de acesso comunicam uns com os outros para conduzir o tráfego de uma BSS para outra, facilitando assim o movimento de estações de uma BSS para outra. Os APs executam esta comunicação através de um meio abstracto que se chama DS. O equipamento de rede fora do ESS, o ESS e todas as estações aparecem como uma única camada MAC. Assim, o ESS esconde a mobilidade das estações de tudo aquilo que está fora do seu limite.

DS - mecanismo pelo qual um *AP* comunica com outro para troca de tramas entre estações.

A figura 3.3 ilustra uma WLAN IEEE 802.11 típica, onde estão incluídos os componentes acima descritos.
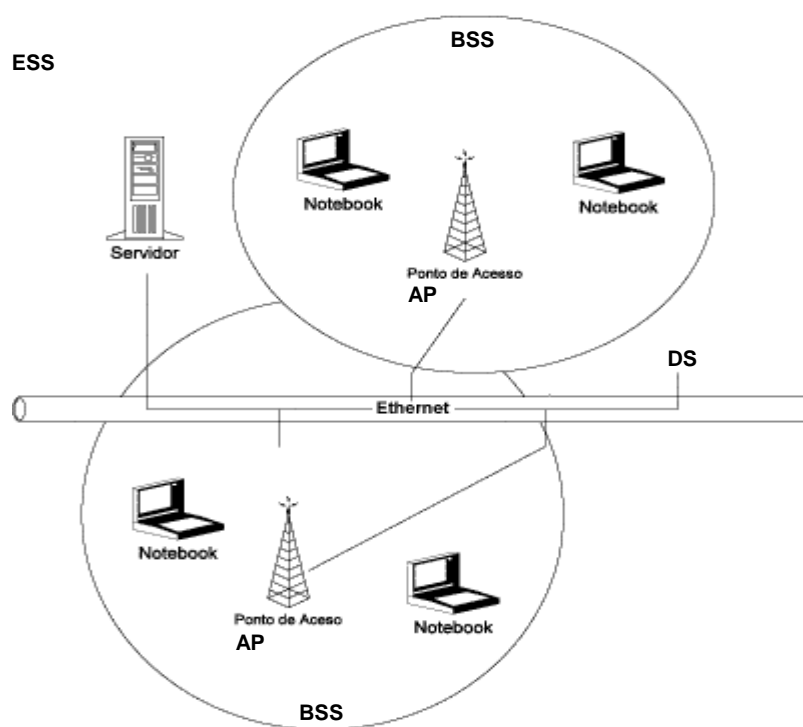
Figura 3.3 - Arquitectura típica de uma rede IEEE 802.11

Arquitectura da *stack*

A *stack* de protocolos do IEEE 802.11 encontra-se ilustrada na figura 3.4 [20].
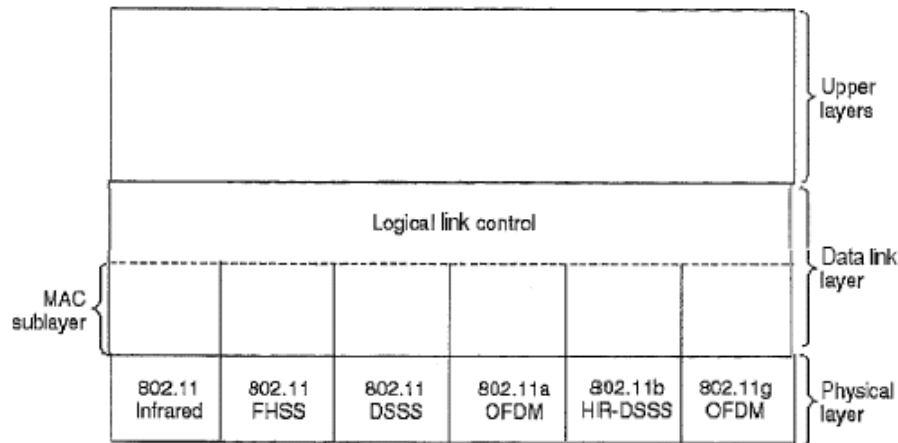
Figura 3.4 - Pilha do protocolo IEEE 802.11

No IEEE 802.11 a camada física tem uma correspondência directa com a camada física OSI, mas a camada de ligação de dados está dividida em duas sub-camadas: a sub-camada MAC e a subcamada LLC (Logical Link Control).

A sub-camada MAC determina como o acesso ao o canal físico é atribuído, ou seja, quem é o próximo a transmitir. A função do LLC é esconder as diferenças entre as variantes do IEEE 802 e torná-las indistinguíveis para o nível seguinte, o nível de rede.

Camada física

O *standard* IEEE 802.11 de 1997 especifica três técnicas de transmissão permitidas pela camada física: um método utiliza tecnologia IR (Infrared) e dois métodos utilizam tecnologia RF de curto alcance, estando todos eles situados na banda não licenciada ISM dos 2,4 GHz. Todos estes métodos permitem velocidades de transmissão de 1 e 2 Mbps. Em 1999 duas novas técnicas de modulação foram introduzidas para permitir uma maior largura de banda: OFDM (nas bandas ISM de 2,4 GHz e 5 GHz) e DSSS (na banda ISM de 2,4 GHz). Estas técnicas permitem velocidades de 54 Mbps e 11 Mbps, respectivamente, muito superiores às velocidades de 1 e 2 Mbps proporcionadas pelo *standard* original.

Cada uma das técnicas permitidas no nível físico permite enviar uma trama de uma estação para outra. Nesta secção efectua-se uma breve referência a cada uma destas técnicas.

A técnica de IR utiliza transmissão difusa, isto é, sem necessidade de linha de vista, sendo permitidas duas velocidades de transmissão de dados: 1 e 2 Mbps. No entanto, existem alguns aspectos negativos, entre eles a não penetração em paredes, tomando esta opção muito pouco popular.

A técnica de modulação FHSS utiliza 79 canais situados na banda ISM dos 2,4 GHz. É utilizado um número pseudo aleatório para produzir a sequência de salto nas frequências. Enquanto todas as estações utilizarem a mesma semente para a criação do número pseudo aleatório e estiverem sincronizadas temporalmente, vão saltar simultaneamente nas frequências. O tempo gasto em cada frequência, o *dwell time*, é um parâmetro ajustável. A técnica FHSS proporciona uma forma muito simples de alocação de espectro. Para além disso, proporciona uma comunicação bastante robusta, uma vez que é insensível à interferência rádio. Esta técnica toma-se bastante popular para interligações entre edifícios. O seu ponto fraco é a baixa largura de banda. A técnica FHSS deixou de ser utilizada nas versões do IEEE 802.11, estando apenas definida no *standard* de 1997.

O terceiro método de modulação definido para a camada física é o método DSSS. Neste método cada *bit* de dados é transmitido através da sua combinação com a sequência de Barker. Esta sequência utiliza modulação da mudança de fase. Podem ser utilizados até 13 canais para transmissão de dados e cada canal possui uma largura de banda de 5 MHz.

A primeira técnica para redes de alta velocidade é a OFDM. Esta técnica utiliza 52 frequências diferentes para comunicação: 48 estão disponíveis para transmissão de dados e 4 para sincronização. Desde que as transmissões estejam presentes em múltiplas frequências ao mesmo tempo, esta técnica é considerada de espalhamento do espectro. Esta técnica é actualmente utilizada nas variantes de alta velocidade do IEEE 802.11.

Camada de Ligação de Dados

A sub-camada MAC do protocolo IEEE 802.11 é um pouco diferente da respectiva camada no protocolo Ethernet. Esta diferença deve-se à complexidade do ambiente sem fios em comparação com o sistema Ethernet baseado na utilização de fios. No protocolo Ethernet uma estação espera que o meio esteja silencioso para começar a transmitir. No protocolo IEEE 802.11 não pode ser utilizado o mesmo esquema, porque numa rede sem fios poderiam surgir dois problemas: a estação escondida e a estação exposta.

No caso do problema da estação escondida, a partir do momento em que todas as estações não estejam no raio umas das outras, podem ocorrer transmissões numa parte da

célula que não são recebidas pelas outras estações. Assim, na situação ilustrada na figura 3.5 [20], a estação C está a transmitir para a estação B, mas se a estação A também quiser transmitir para a estação B, quando escutar o meio vai concluir erradamente que pode transmitir.
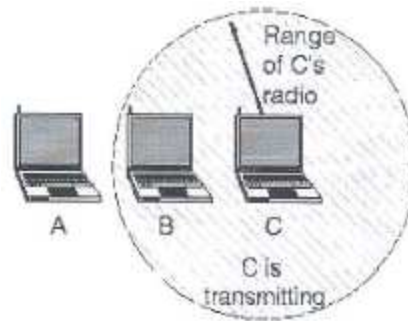
Figura 3.5 - Problema da estação escondida

Em contraste, no caso do problema da estação exposta, para a situação ilustrada na figura 3.6 [20], a estação B pretende enviar uma mensagem para a estação C. Quando escuta o meio conclui erradamente que não pode enviar a mensagem para a estação C, mesmo que A esteja a transmitir para outra(s) outras estação(ões).
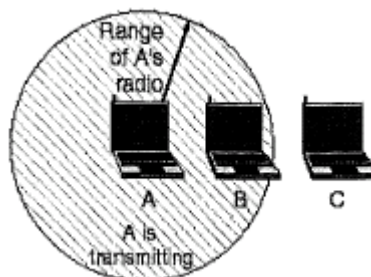
Figura 3.6 - Problema da estação exposta

Para resolver estes problemas o IEEE 802.11 suporta dois tipos de operação: O DCF (Distributed Coordination Function) não utiliza qualquer tipo de controlo central, enquanto o PCF (Point Coordination Function) utiliza uma estação base para controlar toda a actividade na célula. Todos os sistemas devem suportar DCF, mas o modo PCF é opcional.

O modo de operação DCF é utilizado quando o IEEE 802.11 utiliza o CSMA/CA (CSMA with Colision Avoidance), cujo procedimento é o seguinte: a estação que quer transmitir escuta o meio. Se este está livre a estação transmite, não escutando mais o meio enquanto estiver a transmitir. Por outro lado, se o meio estiver ocupado, a estação espera

até que este fique livre e começa então a transmitir. Se ocorre urna colisão, a estação que está a transmitir espera um tempo aleatório, recorrendo a um algoritmo para calcular este tempo, e volta a tentar a transmissão.

O segundo modo de operação é o PCF, no qual a estação base questiona todas as estações para verificar se alguma tem algum pacote para enviar. Uma vez que a transmissão é totalmente controlada pela estação base, nenhuma colisão deve ocorrer. O *standard* define o mecanismo de *polling*, mas não a frequência, a ordem, ou mesmo se todas as estações têm necessidade dos mesmos serviços. O mecanismo básico é a estação base efectuar o *broadcast* de um pacote de aviso periódico. Neste pacote estão registados vários parâmetros do sistema, tais como: sequências de salto, *dwell time* (para FHSS), relógio de sincronização, entre outros.

Outra característica a ter em atenção no modo de operação das WLANs é o tempo de vida da bateria. Uma estação base pode enviar uma estação móvel para o estado de adormecido até que algo aconteça para que esta seja acordada. Entretanto a estação base tem que guardar todos os pacotes dirigidos a essa estação, entregando-lhos quando esta acordar.

Estrutura da trama

O *standard* IEEE802.11 define três tipos de tramas: dados, controlo e gestão. Cada trama é composta por um cabeçalho e por um conjunto de campos utilizados pelo nível MAC. Para além disso existem alguns cabeçalhos usados pela camada física, mas que quase sempre estão ligados às técnicas de modulação implementadas. O formato típico da trama de dados IEEE 802.11 está ilustrado na figura 3.7 [20].
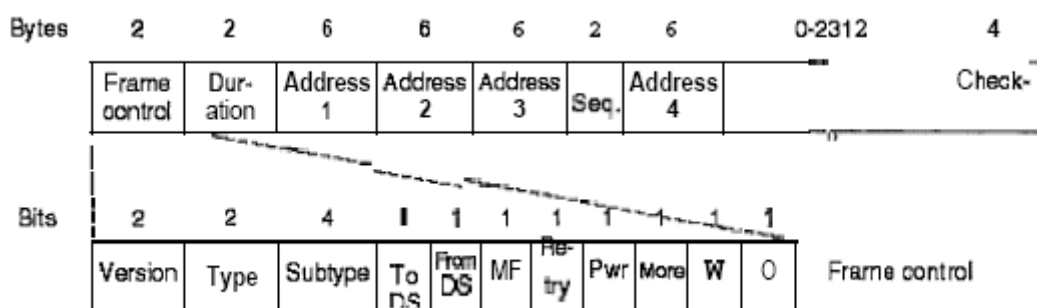
Figura 3.7 - Estrutura típica de uma trama de dados IEEE 802.11

O primeiro campo desta trama é o campo de controlo da trama que é decomposto em 11 campos:

Version (versão do protocolo): tem como função permitir que duas versões do mesmo protocolo estejam a operar ao mesmo tempo na mesma célula;

Type e *Subtype*: têm como funcionalidade a identificação do tipo de trama (dados, controlo ou gestão);

To DS e *From* DS: indica se a trama está a ir para ou a vir do DS (por ex. Ehernet);

MF: significa que mais fragmentos se vão seguir;

Retry: marca a retransmissão de uma trama enviada anteriormente;

Power Management: usado pela estação base para colocar ou retirar o receptor do estado adormecido;

More: indica que o emissor tem tramas adicionais para o receptor;

WEP: especifica se o corpo da trama está encriptado utilizando o algoritmo WEP;

Order: indica ao receptor que a sequência de tramas com este *bit* a 1 deve ser processada com prioridade.

O segundo campo da trama é a Duração (*Duration*), que indica quanto tempo a trama e o aviso de recepção vão ocupar o canal. Este campo também está presente nas tramas de controlo.

O campo seguinte é composto por um conjunto de quatro endereços, todos eles no formato do *standard* IEEE 802: dois são necessários para indicar a origem e o destino da trama, os outros dois servem para indicar a fonte e o destino das estações base que servem de *interface* ao sistema de distribuição.

O campo Sequência *(Sequence)* permite que os fragmentos sejam numerados. Dos 16 *bits* utilizados neste campo 12 identificam a trama e 4 o fragmento.

O campo de dados (*Data*) contém os dados a serem enviados para o receptor. O último campo é o *Checksum* e tem como função a verificação da integridade da mensagem junto do receptor.

As tramas de gestão têm um formato muito similar às tramas de dados, com excepção de um dos endereços de estação base, pois as tramas de gestão são destinadas a uma única célula.

As tramas de controlo são mais pequenas, têm apenas um ou dois endereços, sem campo de dados e de sequência.

Serviços

O *standard* IEEE 802.11 fornece um total de nove serviços. Estes serviços estão divididos em duas categorias: cinco serviços de distribuição e quatro serviços de estação. Os serviços de distribuição estão relacionados com a gestão das estações associadas à célula e com a interacção com outras estações fora da célula. Em contraste os serviços de estação estão relacionados com a actividade interna da célula.

Os cinco serviços de distribuição são fornecidos pela estação base e estão ligados à mobilidade de uma estação, isto é, como a estação entra e sai de uma célula, ligando-se e desligando-se das estações base. Os serviços de distribuição são os seguintes:

Associação

Este serviço é utilizado pelas estações móveis para se ligarem às estações base. Tipicamente é usado depois de uma estação se mover dentro do raio de rádio da estação base. Após a sua chegada, anuncia a sua identidade e capacidades. As capacidades incluem as taxas de dados suportadas, necessidade de serviços e gestão de energia. A estação base pode aceitar ou rejeitar a estação móvel. Se a estação móvel for aceite deve em seguida autenticar-se.

Desassociação

Tanto a estação móvel como a estação base podem desassociar-se, quebrando a relação que mantêm. Uma estação deve usar este serviço antes de se desligar ou sair. A estação base deve usar igualmente este serviço antes de se desligar para manutenção.

Reassociação

Uma estação pode mudar a sua estação base utilizando este serviço. É bastante útil para uma estação que se está a mover de uma célula para outra. Se for utilizado correctamente nenhum dado será perdido com a alteração.

Distribuição

Este serviço determina como a tramas são encaminhadas até à estação base. Se o destino for local à estação base, as tramas podem ser enviadas directamente através do ar. De outra forma, terão que ser encaminhadas por uma rede de fios.

Integração

Se a trama de dados tiver que ser enviada para uma rede que não seja IEEE 802.11 com um esquema diferente de endereços ou de formatos, este serviço toma conta da transição entre o formato IEEE 802.11 e o formato requerido pela rede de destino.

Os restantes quatro serviços são intra-célula, sendo requeridos após a associação estar estabelecida.

Autenticação

Uma vez que as comunicações sem fios podem ser facilmente recebidas por estações não autorizadas, uma estação deve ser autenticada antes de iniciar o envio de dados. Após a associação da estação móvel à estação base, isto é, após a estação móvel ser aceite na célula, a estação base envia uma trama especial de descoberta para verificar se a estação móvel conhece a chave secreta com que foi programada. Para provar o conhecimento desta chave a estação móvel tem que encriptar a trama de descoberta e reenviá-la para a estação base. Se o resultado estiver correcto a estação móvel passa a fazer parte da célula.

Desautenticação

Se uma estação previamente autenticada pretende abandonar a rede é desautenticada. Após a conclusão deste serviço não poderá voltar a utilizar a rede.

Privacidade

Para a informação ser enviada através de uma LAN sem fios e continuar confidencial deve ser encriptada. Este serviço é responsável pela encriptação e desencriptação. O algoritmo utilizado para a encriptação é o algoritmo RC4.

Entrega de dados

Como o *standard* IEEE 802.11 foi modelado sobre a Ethernet e as transmissões sobre esta não são garantidas a 100%, a transmissão sobre IEEE 802.11 também não é garantida. As camadas superiores devem detectar e corrigir os erros originados.

Segurança

Uma rede sem fios é menos segura do que uma rede com fios. Se a rede sem fios for desenvolvida sem segurança pode resultar numa perda da qualidade de serviço, ou até

mesmo no seu uso como ponto de partida para ataques. Existem diversos procedimentos cujo objectivo é a resolução de problemas de segurança, que permitem tornar a rede sem fios mais segura e imune a ataques.

O protocolo IEEE 802.11 providencia mecanismos de autenticação, confidencialidade, controlo de acessos e integridade de dados, para que estranhos à rede não possuam autorização de utilização dos seus serviços. Alguns desses mecanismos são a seguir analisados.

SSID

O SSID (Service Set IDentifier) actua como uma simples palavra-chave, uma vez que tem de ser apresentado pela estação cliente ao AP. Esta medida de segurança pode ser comprometida se o AP estiver configurado para transmitir o SSID em *broadcast*, já que qualquer cliente, mesmo não configurado, está apto a receber o SSID. Para que este problema não aconteça, o AP deve estar configurado para não efectuar *broadcast* do SSID, ou seja, operar em modo fechado.

O acesso à BSS é realizado utilizando um SSID único associado com um AP ou um grupo de APs. O SSID proporciona um mecanismo de segmentação da rede sem fios em múltiplas redes servidas por um ou vários APs. Cada AP é programado com um SSID e para aceder ao AP a estação cliente deve ser configurada com o SSID correcto.

Para a estação cliente poder aceder de diversas localizações é configurada com múltiplos SSIDs para as diferentes localizações. Não deve ser permitido o acesso de um dispositivo que não tenha o SSID correcto. A utilização de SSID é a forma mais básica de segurança numa rede sem fios. No entanto, os problemas são inúmeros e o nível de segurança proporcionado muito baixo. Para resolver estes problemas foram desenvolvidas outras formas de aumentar a segurança.

WEP

Um dos métodos para aumentar a segurança na comunicação e integridade dos dados nas WLANs é a utilização do protocolo de segurança de dados WEP. O WEP proporciona um método de encriptação implementado na subcamada MAC. A sua principal funcionalidade é a prevenção de acessos não autorizados. O WEP apenas é utilizado na comunicação entre as estações e os APs. Após a entrada da trama na rede, este mecanismo deixa de estar acessível

A integridade deste algoritmo é baseada nos 32 *bits* do *Checksum*, situados no final da trama MAC (Figura 3.7), [20]. No processo de encriptação existe uma chave secreta de 40 ou 64 *bits* que é partilhada entre os dois participantes. A esta chave de encriptação é concatenado um vector de inicialização de 24 *bits.* O bloco resultante forma a semente que irá ser a entrada para o gerador de números pseudo aleatórios (PRNG - Pseudo Random Number Generator) definido no algoritmo RC4. O PRNG gera uma sequência de *bits* do mesmo tamanho da trama MAC mais o *Checksum.* Em seguida através de um OR exclusivo *bit* a *bit* entre a trama MAC e a sequência produzida pelo PRNG é produzido o texto decifrado. O vector de iniciação é adicionado à trama MAC antes da sua entrada no bloco OR. O vector de iniciação é modificado periodicamente (praticamente em todas as transmissões). Cada vez que este é modificado, a sequência do PRNG também é modificada, dificultando a descodificação da trama.

Após a recepção da trama o receptor recupera o vector de iniciação do bloco de dados e concatena este com a chave secreta partilhada para gerar a mesma sequência usada pelo transmissor. Em seguida é efectuado um XOR entre a chave e o bloco de dados com o objectivo de recuperar os dados originais. Finalmente, o receptor compara o *Checksum* que recebeu com o *Checksum* calculado no receptor para validar a integridade dos dados.

Com o objectivo de aumentar o nível de segurança neste algoritmo, foi adicionado aos 40 *bits* da chave secreta partilhada um vector de inicialização único formado por 24 *bits*. Assim, em vez dos 40 *bits* de chave partilhada passa-se a ter 64 *bits*, no entanto o receptor apenas tem de conhecer a chave secreta de 40 *bits*. Os restantes 24 *bits* do vector de inicialização são transmitidos não encriptados e determinam somente qual a chave que está a ser utilizada para encriptar os pacotes.

Apesar de todos estes processos para aumentar o nível de segurança, este tem muitas falhas: número finito de vectores de inicialização, não existência de nenhum mecanismo para troca de chaves secretas quando todos os vectores de inicialização estão a ser usados e processo de concatenação do vector à chave demasiado simples, produzindo chaves únicas muito similares [20]. No entanto, apesar de o WEP ter muitos problemas é melhor activar este procedimento de segurança do que a rede estar exposta a ataques, sem qualquer sistema de segurança. Para resolver os problemas ocorridos com o WEP alguns fabricantes resolveram aumentar o número de *bits* utilizados para 152 ou 256. No entanto, este procedimento não resolve os problemas de segurança, apenas aumenta o tempo gasto a tentar quebrar a segurança do WEP.

Filtro de endereços MAC

Um AP ou grupo de APs pode ser identificado por um SSID, no caso de uma estação cliente poder ser identificada pelo endereço MAC da sua carta de rede IEEE 802.11. Para aumentar a segurança da rede, cada AP pode ser programado com uma lista de endereços MAC associados, com permissão para aceder a esse AP. Se o endereço MAC da estação cliente não estiver na lista não lhe é permitido associar-se com esse AP. O filtro de endereços MAC, em conjunto com o SSID, aumenta a segurança da rede. Mas este método só é viável para pequenas redes em que a lista de endereços MAC possa ser gerida facilmente. Cada AP tem que ser programado manualmente com a lista de endereços MAC e esta deve ser mantida actualizada.

VPN

As soluções VPN (Virtual Private Network) foram desenvolvidas como uma forma de acesso seguro a uma rede via Internet pública. A VPN proporciona um caminho seguro e dedicado (túnel) para aceder à rede através de um caminho não seguro. Vários protocolos de túnel (PPTP e L2TP) são usados em conjunto com soluções de autenticação centralizadas tais como o servidor RADIUS.

Os APs são configurados para proporcionar acesso livre, sem encriptação WEP, mas isolados da rede da empresa através do servidor VPN. A autenticação, encriptação e confidencialidade na rede sem fios são proporcionadas através dos servidores VPN, que também actuam como *firewalls*/*gateways* para a rede privada. Uma solução deste tipo tem várias vantagens, sendo de destacar as seguintes: são escaláveis a qualquer número de estações cliente; têm uma baixa necessidade de administração, que está centralizada nos servidores VPN e o WEP e o filtro de endereços MAC não são necessários, pois a segurança é criada pela própria VPN.

As soluções VPN são boas para as redes que já possuam uma infra-estrutura para acesso remoto. No entanto, e apesar de esta ser uma boa forma de segurança para a rede, estão a emergir métodos alternativos baseados no *standard* IEEE 802.11i.

3.4.2 IEEE 802.15.1/Bluetooth

O Bluetooth foi originalmente desenvolvido com o objectivo de substituir a cablagem na interligação de dispositivos electrónicos fixos ou móveis. As suas características principais são: robustez, baixa complexidade, baixo consumo e baixo custo.

Para além destas características oferece possibilidade de ligação a LANs, PANs, redes de telemóveis e Internet.

Para que esta tecnologia fosse ainda mais atractiva, o Bluetooth SIG (Special Interest Group) colocou-a na largura de banda não licenciada ISM de 2.4 GHz, o que permite a sua utilização sem custos adicionais no que concerne à utilização da largura de banda.

Uma das chaves do sucesso do Bluetooth é a procura da harmonização das comunicações entre os diversos fabricantes para que os seus equipamentos possam comunicar sem problemas uns com os outros. Para o conseguir, o Bluetooth define, não só a arquitectura rádio, mas a camada de *software* que permite às aplicações que correm nesses dispositivos encontrarem outros dispositivos Bluetooth na área, descobrirem os serviços que oferecem e utilizá-los.

A figura 3.8 [20] ilustra a relação entre o modelo de referência OSI e o modelo de referência do protocolo Bluetooth. O Bluetooth não corresponde exactamente ao modelo OSI, mas é possível relacionar os níveis Bluetooth com os níveis equivalentes no modelo OSI.
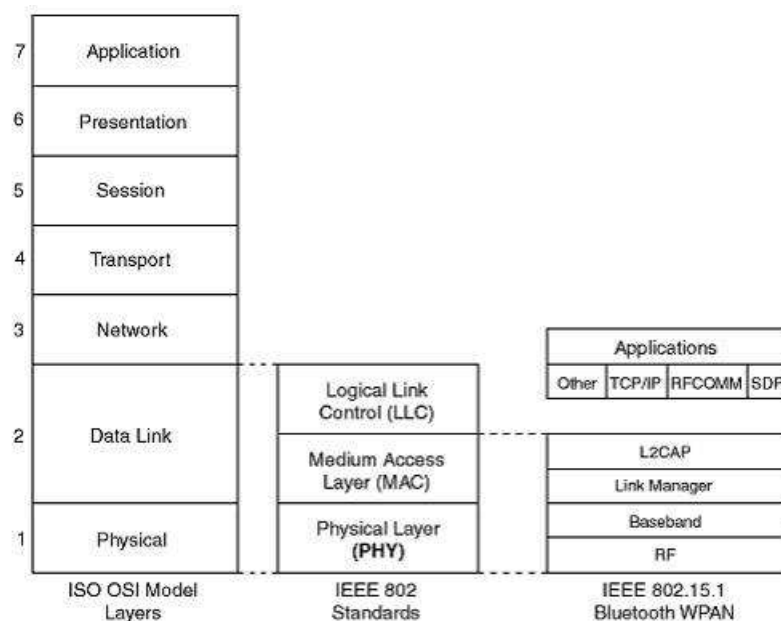
Figura 3.8 - O modelo de referência OSI, os *standard*s IEEE 802 e o Bluetooth

O protocolo Bluetooth é definido como uma série de camadas, embora existam algumas características que são inter-camadas (Figura 3.9) [22].
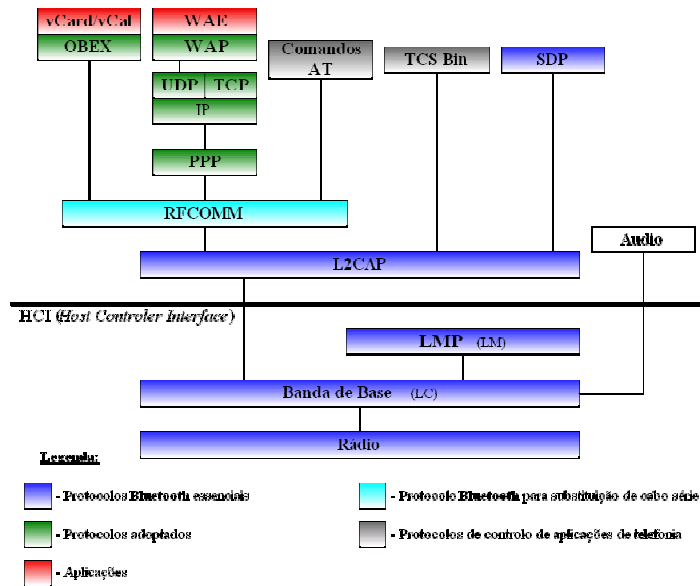
Figura 3.9 - Pilha de protocolos Bluetooth

A especificação Bluetooth é constituída por duas partes: o núcleo e os perfis. Estas irão ser analisadas em seguida.

Núcleo

A especificação do núcleo consiste nos quatro níveis mais baixos do modelo, bem como pelo nível de serviço SDP (Service Discovery Protocol) (Figura 3.9).

A camada rádio é a camada mais baixa na pilha de protocolos. A especificação da sua *interface* define as características do rádio, bandas de frequência de funcionamento, arranjo de canais, níveis de potência de transmissão e níveis de sensibilidade de recepção.

Em seguida, a camada *Baseband* tem como função o transporte do processamento do nível físico e do nível MAC. Este processamento inclui tarefas como: descoberta de dispositivos, formação de ligações e comunicação síncrona e assíncrona entre dispositivos.

Os dispositivos Bluetooth devem trocar algumas mensagens de controlo com a função de configuração e gestão das ligações. As definições das mensagens fazem parte do protocolo LMP (Link Manager Protocol). A entidade funcional responsável por transportar o processo associado ao LMP é o LM (Link Manager).

O L2CAP (Logical Link Control and Adaptation Protocol) pode ser visto como a camada de ligação do Bluetooth. Usualmente, o L2CAP e os níveis acima deste são implementados em *software*. O L2CAP tem como função a entrega dos pacotes recebidos de níveis mais elevados ao outro lado da ligação. Os dispositivos Bluetooth podem

estabelecer uma ligação L2CAP tão cedo quanto estes estiverem no raio um do outro. O dispositivo cliente em seguida necessita de descobrir os serviços prestados pelo dispositivo servidor.

O SDP define o meio pelo qual o dispositivo cliente pode descobrir os serviços, bem como os seus atributos. O desenho do SDP foi optimizado para o Bluetooth e define unicamente os mecanismos de descoberta. Os métodos de aceder a esses serviços estão fora do seu domínio.

Em seguida descreve-se mais pormenorizadamente cada uma destas camadas.

Rádio

O Bluetooth opera na banda ISM dos 2.4 GHz, a qual está disponível para uso sem necessidade de licença.

O Bluetooth utiliza um esquema de FHSS bastante rápido, num total de 79 canais, tendo cada canal uma largura de banda de 1 MHz. A máxima frequência de saltos deste esquema é 1.6 KHz, que corresponde ao comprimento de *slot* de 625 μs. Para cada pacote enviado é escolhida uma nova frequência para o seu envio, o que resulta numa taxa de 1600 saltos/s. Consegue-se desta forma uma boa imunidade a outras fontes de interferência presentes. Na versão 1.2 foi introduzido um esquema adaptativo, o AFH (Adaptive Frequency Hopping), que permite a exclusão de portadoras (canais) caso seja verificada corrupção de pacotes nessas frequências O AFH é utilizado com o objectivo principal de melhorar a *performance* de uma *piconet* na presença de outros sistemas *nonhopping* na banda 2.4 GHz, mas também como uma maneira de melhorar a *performance* entre *piconets* coexistentes.

Os dados são modulados segundo o esquema GFSK (Gaussian Frequency Shift Keying), sendo a velocidade máxima de transferência de dados de 1 Mbps. Na versão 2.0 foi introduzida uma melhoria na taxa de transmissão de dados, ao serem utilizados esquemas de modulação de dados DPSK (Differential Phase Shift Keying) e DQPSK (Differential Quadrature Phase Shift Keying). A taxa de transmissão é cerca de 3 vezes mais rápida do que nas versões anteriores.

Cada dispositivo Bluetooth está classificado numa de três classes de potência, classe 1, 2 ou 3 (Tabela 3.1) [22].

A classe 1 integra os dispositivos de longo alcance (~100 m) com uma potência de saída máxima de 100 mW (20 dBm). A classe 2 compreende os dispositivos de alcance

médio (~10 m) com uma potência máxima de saída de 2.5 mW (4 dBm). Na classe 3 estão incluídos os dispositivos de curto alcance (~10 cm) com uma potência máxima de saída de 1 mW (0 dBm).

Tabela 3.1 - Classes de potência Bluetooth

	Potência mínima	Potência máxima	Alcance
Classe 1	0 dbm (1 mW)	20 dbm (100 mW)	100 m
Classe 2	-6 dbm (0.25 mW)	4 dbm (2.5 mW)	10 m
Classe 3	-30 dbm (1 µW)	0 dbm (1 mW)	1 m

Tipicamente os dispositivos Bluetooth pertencem à classe de potência 1. Quando são utilizados dispositivos de classe 2, com uma potência de transmissão de 20 dBm, isso resulta num maior alcance, mas requer a implementação de mecanismos de controlo de potência para garantir as regras de partilha da banda ISM.

Banda de base

Esta camada forma, em conjunto com o rádio, o nível físico do Bluetooth. As suas principais funções são: fornecimento das sequências de salto, encriptação de baixo nível para a criação de ligações seguras, manuseamento dos pacotes de dados sobre a ligação sem fios, gestão das ligações síncronas e assíncronas e correcção de erros. O *transceiver* desta camada utiliza um esquema TDD (*Time Division Duplex*) com o objectivo de poder transmitir e receber alternadamente.

Topologia

As redes Bluetooth são organizadas em *piconets*, onde uma unidade *master* coordena o tráfego de e para um máximo de sete unidades *slave* activas. O *master* manda o request para possibilitar o estabelecimento de uma ligação. Na *piconet* as várias unidades *slave* apenas podem comunicar umas com as outras através do *master*. Cada unidade Bluetooth pode pertencer simultaneamente a quatro diferentes *piconets*, podendo no entanto ser *master* apenas numa. As *piconets* estão interligadas numa scaternet (figura 3.10) [22].
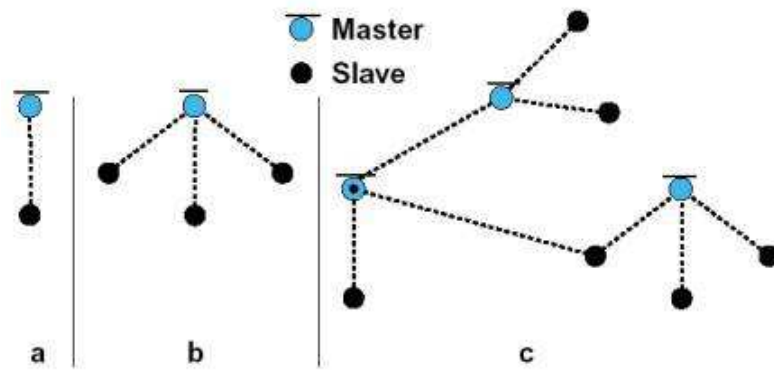
Figura 3.10 - Topologia de uma rede Bluetooth
a) *piconet* com um *slave*; b) *piconet* com múltiplos *slaves*; c) *scaternet*

Tipos de Ligações

É feita uma distinção entre dois tipos de ligações: ACL (Asynchronous Connectionless Link) para a transmissão de dados e SCO (Synchronous Connection Oriented) destinadas à transmissão de voz.

Uma ligação ACL é uma ligação ponto a multiponto entre o *master* e todos os *slaves* participantes na *piconet.* O *master* pode estabelecer uma ligação ACL nos espaços não reservados para as ligações SCO. Só pode existir uma ligação ACL de cada vez. A retransmissão é permitida e é essencialmente utilizada para transferência de dados.

As ligações ACL asseguram uma transmissão de dados fiável e segura com um esquema ARQ (Automatic Repeat reQuest), o qual inicia a retransmissão de um pacote no caso de a avaliação do CRC (Cyclic Redundancy Check) incluído mostrar inconsistências. Isto assegura a recepção de informação livre de erros.

A ligação SCO é uma ligação simétrica ponto a ponto entre o *master* e um *slave* numa *piconet.* O *master* mantém a ligação SCO reservando espaço em intervalos regulares. A principal função deste tipo de ligação é o transporte de voz. Um mestre pode suportar até três ligações SCO.

As ligações SCO suportam tráfego em tempo real ao reservar *slots* de tempo em intervalos de tempo periódicos. Nas versões anteriores não eram permitidas retransmissões neste tipo de ligação, mas na versão 1.2 foram introduzidas melhorias nas ligações SCO, de modo a possibilitar a existência de um número limitado de retransmissões. A ligação SCO *extended* é bastante flexível, suportando várias taxas de transmissão.

Estrutura dos pacotes

Para os dados circularem num canal Bluetooth têm que ser convertidos em pacotes. O formato geral deste pacote está ilustrado na Figura 3.11 [20]. Cada pacote é constituído por 3 entidades: o código de acesso (Access *Code)*, o cabeçalho (Header) e o corpo (Playload).

Figura 3.11 - Formato de um pacote Bluetooth

Código de Acesso

É utilizado para sincronização temporal, compensação de offset, inquirição e numeração. Existem três tipos diferentes de códigos de acesso: CAC (Channel Access Code), DAC (Device Access Code) e IAC (Inquiry Access Code).

O CAC identifica de uma forma única a *piconet*. O DAC é utilizado para procedimentos especiais de sinalização, como o *paging* e a resposta a *paging*. O IAC é utilizado em acções de inquirição.

Cabeçalho

Contém informação para o reconhecimento do pacote, número do pacote para reordenação no caso de recepção dos pacotes fora de ordem, controlo do fluxo, endereço do *slave* e correcção de erros do cabeçalho.

Corpo

Contém os campos de voz ou de dados. Se for um campo de dados, este contém um cabeçalho. Os pacotes ACL têm campo de dados, enquanto os pacotes SCO apenas contêm campo de voz.

Existem seis tipos de pacotes ACL que podem ocupar um, três ou cinco *slots* de tempo, dependendo do tipo utilizado. Três tipos de pacotes ACL incluem um corpo não codificado, enquanto os outros três têm o corpo protegido por FEC (Forward Error Correction) com uma taxa de 2/3. Os três tipos de pacotes ACL não codificados são conhecidos por DH1, DH2 e DH3, enquanto os três codificados são DM1, DM3 e DM5.

Utilizando os pacotes do tipo DM5 para dados e DH1 para *acknowledge* resulta na máxima taxa de transmissão possível (unidirecional) para o Bluetooth, a 723 Kbps.

Existem três diferentes tipos de pacotes SCO, que têm o mesmo comprimento e requerem um *slot* de tempo de transmissão de 625 μs. Tipicamente transportam 64 Kbps de voz codificada CVSD (Continuous Variable Slope Delta). Tal como os pacotes ACL, os pacotes SCO são diferenciados pela codificação utilizada: os HV1 têm um código de repetição com uma taxa de 1/3, os HV2 são codificados por FEC com uma taxa de 2/3, enquanto os HV3 não são codificados. Numa ligação HV1 os pacotes são transmitidos em todos os segundos *slots* de tempo (o que significa que numa ligação deste tipo nenhum outro tráfego pode ser transmitido na *piconet*), numa ligação HV2 os pacotes são transmitidos em todos os quartos *slot*s de tempo e numa ligação HV3 os pacotes são transmitidos em todos os sextos *slots* de tempo. Os pacotes SCO perdidos podem ser recolocados através de uma *erasure pattern*.

O código de acesso e o cabeçalho têm um tamanho fixo: 72 e 54 *bits* respectivamente. O corpo do pacote tem um tamanho que pode variar desde 0 até ao máximo de 2745 *bits*. Podem existir diferentes tipos de pacotes, sendo alguns compostos apenas pelo código de acesso, outros pelo código de acesso e cabeçalho e ainda outros pelo código de acesso, cabeçalho e corpo.

Modos de Ligação

Um dispositivo Bluetooth, após o estabelecimento de uma ligação, pode ficar num dos seguintes modos:

Modo Activo

Neste modo, a unidade participa activamente no canal. O *master* efectua um escalonamento das transmissões baseado no tráfego vindo de cada *slave* e efectua transmissões regulares para manter os escravos sincronizados com o canal. Os *slaves* activos escutam o meio durante os *slots* de tempo reservados aos pacotes *master*-to-*slave*, os que não estiverem endereçados podem adormecer até à próxima transmissão do *master*.

Modo Espera

Os dispositivos sincronizados com a *piconet* podem entrar em modo de poupança de energia, durante o qual a actividade do dispositivo é baixa. Neste modo o dispositivo escuta a *piconet* a uma taxa muito baixa. O intervalo de espera é programável e depende da

aplicação. Este modo tem o duty cycle mais alto, logo é o mais eficiente em termos de poupança de energia.

Modo Suspenso

Os dispositivos sincronizados com a *piconet* entram em modo de poupança de energia. Os *master*s podem colocar os *slaves* em modo suspenso, mantendo apenas activo um temporizador interno. Os *slaves* também podem pedir para entrar em modo suspenso. A transferência de dados inicia-se instantaneamente quando as unidades transitam para fora deste modo.

Modo Parqueado

Neste modo os dispositivos estão sincronizados com a *piconet* mas não participam no tráfego. Estes dispositivos escutam ocasionalmente o tráfego do *master* para se sincronizarem e escutarem mensagens de *broadcast*. Este é o modo que tem o *duty cycle* mais baixo, logo é o menos eficiente em poupança de energia.

LMP

A função desta camada é a organização das ligações e sua configuração. O LMP consiste essencialmente num número de PDUs que são enviadas de um dispositivo para o outro indicado no cabeçalho do pacote. Os PDUs são enviados sempre como pacotes de um só espaço, sendo o corpo constituído apenas por um *byte*. O LMP possui funcionalidades para prender e desprender escravos, trocar regras entre um mestre e um escravo e estabelecer ligações ACL ou SCO. Efectua a gestão dos modos de ligação com o objectivo de economizar energia quando o dispositivo não tem dados para enviar.

As tarefas de configuração de ligações incluem o ajuste dos parâmetros de ligação, qualidade de serviço e controlo de energia. A autenticação dos dispositivos que vão fazer parte da *piconet* é também função desta camada.

A principal função do HCI (Host Controller Interface) é proporcionar uma *interface* de comando para o controlador da banda de base e gestor de ligações. Permite ainda aceder ao estado do *hardware* e do controlo dos registos. Esta *interface* proporciona um método uniforme de aceder às capacidades da banda de base.

L2CAP

As principais funções desta camada são: multiplexação, segmentação, reassemblagem e QoS.

Na multiplexação o protocolo deve permitir que múltiplas aplicações utilizem simultaneamente uma ligação entre dois dispositivos.

Na segmentação o protocolo deve reduzir o tamanho dos pacotes enviados pelas aplicações para o tamanho aceite pela banda base.

O L2CAP permite que as aplicações tenham uma QoS em certos parâmetros. Verifica se a ligação é capaz de suportar essa QoS e, se tal for possível, proporciona-o. Basicamente o L2CAP trata do nível de rede para as aplicações e protocolos mais elevados.

SDP

O Bluetooth foi desenvolvido com o objectivo de ser implementado em dispositivos com mobilidade. Isto significa que os dispositivos têm de descobrir e serem descobertos por novos dispositivos enquanto estão em movimento. Para tal, o Bluetooth inclui um protocolo de descoberta de serviços de dispositivos, o SDP. O dispositivo que oferece um serviço através do SDP é o servidor SDP e o dispositivo que está à procura de um serviço SDP é um cliente SDP. A base de dados SDP é basicamente um conjunto de entradas que descreve todos os serviços disponibilizados por um dispositivo Bluetooth. Cada serviço na base de dados tem atributos associados a si. Um atributo contém três partes: tipo de dados, tamanho dos dados e os próprios dados. Para o serviço de descoberta ser mais simples existe uma estrutura hierárquica. Os clientes começam por examinar o caminho e depois procuram até encontrar o serviço desejado. O serviço também pode ser acedido directamente através do seu UUID (*Universally Unique Identifier*). Se um fabricante pretende desenvolver um novo serviço e disponibilizá-lo na base de dados SDP, pode incluir o seu próprio UUID nesta base de dados. O processo de construir um UUID está definido, logo o UUID vai ser único, não entrando em conflito com outros serviços.

Perfis

Os fabricantes podem usufruir dos serviços oferecidos pela camada de protocolos Bluetooth para criar uma grande variedade de aplicações. Como o factor interoperabilidade é fundamental na operação do Bluetooth, foram definidas especificações de perfis para o

suportarem. Os perfis especificam parâmetros de controlo e de camada, bem como características e procedimentos necessários para a interligação de dispositivos Bluetooth. A variedade de modos de utilização Bluetooth significa que os dispositivos podem ser chamados por uma grande variedade de protocolos e funções. Para assegurar que todos os modos de utilização trabalham com os dispositivos de outros fabricantes, existe um conjunto de protocolos e funções que foram standardizadas. A presente especificação contém vários perfis (Figura 3.12) [22]. Os perfis mais implementados serão abordados nas subsecções seguintes.
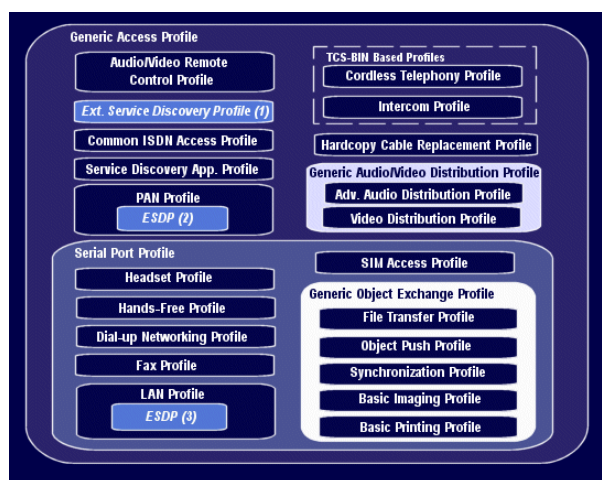
Figura 3.12 - Estrutura de perfis Bluetooth

Generic Access Profile

Define o modo como os dispositivos Bluetooth se descobrem e ligam uns aos outros e quais os protocolos de segurança que utilizam. Todos os dispositivos devem estar em conformidade pelo menos com este perfil para assegurar a interoperabilidade básica entre si.

Service Discovery Aplication Profile

O perfil SDAP utiliza partes do General Access Profile para definir o modo de descoberta dos serviços Bluetooth. O serviço de descoberta define os protocolos e procedimentos que devem ser utilizados pela aplicação de descoberta.

Cordless Telephony Profile

Este perfil define os procedimentos necessários para a interoperabilidade entre diferentes unidades activas no modo de utilização "telefone 3 em 1".

Serial Port Profile

Define a forma de configurar e ligar portas série virtuais entre dois dispositivos. Esta emulação do cabo série pode ser utilizada para tarefas de transferência de dados e impressões.

Generic Object Exchange Profile

É utilizado por aplicações para manusear trocas de objectos. Esta capacidade é depois utilizada por outros perfis para troca de objectos, ficheiros e sincronização.

Object Push Profile

Troca de pequenos objectos, tais como cartões electrónicos.

File Transfer Profile

Transferência de ficheiros entre dois dispositivos Bluetooth.

Synchronization Profile

Sincronização de calendários e informação de endereços entre dispositivos.

Segurança

Uma vez que os dados são transportados através de ondas rádio, qualquer pessoa com o equipamento correcto pode obter esses dados. Para proporcionar segurança e confidencialidade na transferência de dados, foram implementadas medidas de segurança no nível de aplicação e no nível de ligação de dados. Isto significa que em cada dispositivo estão implementadas rotinas de autenticação e de encriptação. Para manter a segurança numa ligação Bluetooth são especificadas várias formas de segurança: endereço do dispositivo, chaves secretas e um número pseudo aleatório que é regenerado em cada transferência. Em seguida são analisadas as diferentes formas de segurança.

O endereço do dispositivo é composto por 48 *bits* e pode ser obtido através de interacções ou através de uma rotina. As chaves secretas são obtidas na inicialização e, após este passo, não são modificadas até terminar o processo de comunicação. A chave de encriptação é obtida a partir da chave de autenticação, durante o processo de autenticação. O tamanho da chave utilizada no algoritmo de autenticação é de 128 *bits*.

No algoritmo de encriptação o tamanho da chave pode variar entre 1 e 6 octetos (8 a 128 *bits*). A chave de encriptação é diferente da chave de autenticação, pois cada vez que a encriptação é activada uma nova chave é gerada. Assim, o tempo de vida da chave de encriptação não corresponde ao tempo de vida da chave de autenticação. O número pseudo aleatório utilizado nas chaves de autenticação e de encriptação para aumentar o nível de segurança é derivado de um processo pseudo aleatório.

O processo de segurança requer um PIN secreto que tem que ser conhecido do utilizador para este aceder a um determinado dispositivo. O processo de segurança é o seguinte (Figura 3.13):

Geração de uma chave de inicialização utilizando o PIN, o tamanho deste, um número aleatório e o endereço do dispositivo;

O processo de autenticação é efectuado com recurso a um esquema de resposta a partir de um desafio. A unidade de verificação envia um número aleatório gerado por um processo para a autenticação. Este número é tal que o dispositivo que tem a chave correcta de inicialização e o endereço correcto vai produzir um número de resposta e enviá-lo para ser verificado;

A chave de encriptação é gerada a partir da chave de ligação. Ambos os dispositivos podem gerar esta chave, que é utilizada para encriptar os dados. O código de acesso e o cabeçalho nunca devem ser encriptados. Se for estabelecida outra ligação entre estes dispositivos a chave de ligação pode ser recordada, evitando a repetição de todo o processo de envio de chaves.
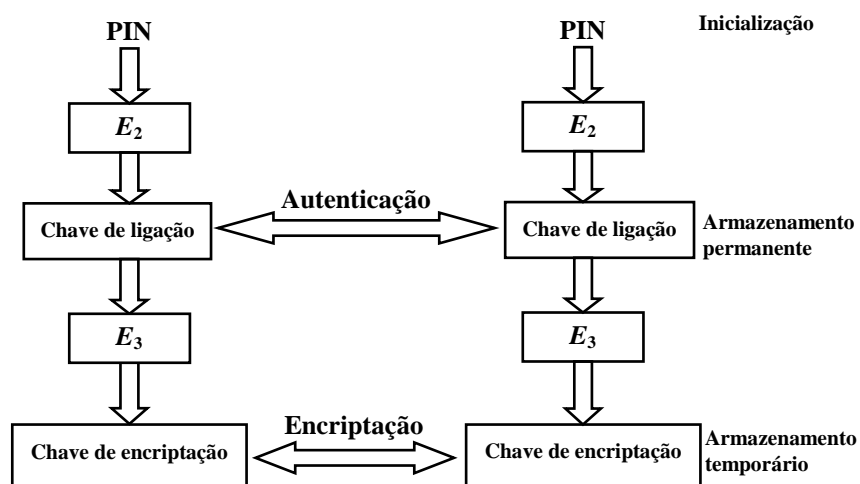
Figura 3.13 - Arquitectura de segurança Bluetooth

3.4.3 IEEE 802.15.4/Zigbee

O *standard* IEEE 802.15.4 foi finalizado em Outubro de 2003 e especifica as características da camada física e da sub-camada MAC de uma *stack* de uma rede de rádio (Figura 3.14) [27]. O objectivo do *standard* IEEE 802.15.4 era a criação de uma solução de comunicação sem fios de dois sentidos, de baixo custo e muito baixo consumo de energia, que satisfizesse os requisitos únicos dos componentes envolvidos (sensores, actuadores e controladores).
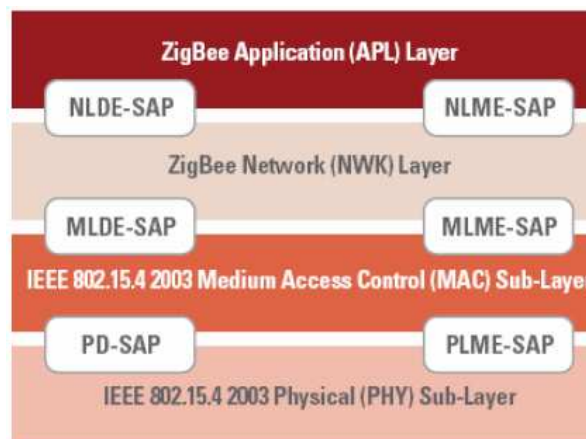
Figura 3.14 - Arquitectura da *stack* de protocolo IEEE 802.15.4/Zigbee

A especificação Zigbee foi finalizada em Dezembro de 2004 e descreve os protocolos das camadas mais altas (rede e aplicação) que operam acima do IEEE 802.15.4. Foi elaborada por um consórcio entre a indústria e instituições de investigação, o consórcio Zigbee, que tinha como objectivo a elaboração de um protocolo para os seguintes mercados: controlo de casas e edifícios, controlo industrial, segurança, electrónica de consumo, periféricos de PC, monitorização médica, bem como controlo de brinquedos e de jogos. Estas aplicações geralmente requerem grande duração de bateria, fiabilidade, possibilidade de adicionar e remover nós da rede facilmente.

Em contraste com o Bluetooth e o IEEE 802.11, esta norma foi desenvolvida especificamente para a utilização em aplicações com muitos componentes pouco utilizados e que transmitem pacotes de dados muito pequenos. Ora estes são os requisitos típicos das redes de campo.

O protocolo IEEE 802.15.4/Zigbee distingue dois tipos de componentes, de acordo com as suas funcionalidades: um FFD (Full Function Device) e um RFD (Reduced Function Device).

Um FFD implementa a *stack* do protocolo IEEE 802.15.4/Zigbee completa. Pode ser coordenador da rede e pode trabalhar com outros FFDs numa ligação ponto-a-ponto;

UM RFD implementa apenas uma parte da *stack* do protocolo IEEE 802.15.4/Zigbee. Um RFD tem de estar sempre associado a um FFD e está limitado à troca de dados apenas com esse FFD.

O Zigbee distingue três tipos de componentes numa rede, de acordo com o papel por eles desempenhado na própria rede: o coordenador, o *router* e o *end device*.

O coordenador é um FFD. É o componente controlador da PAN, isto é, tem a responsabilidade de iniciar e configurar a formação da rede. Apenas existe um coordenador em cada rede e depois de a rede estar formada pode exercer as funções de um *router*.

O *router* é um FFD. Participa no encaminhamento de mensagens. Pode associar-se ao coordenador da rede, a outros *router*s, ou ainda a *end device*s.

O *end device* pode ser um RFD. Está associado a um *router*, não permite a associação de outros componentes, nem participa no encaminhamento de pacotes de dados. É apenas um nó sensor ou actuador.

Topologia da rede

O protocolo IEEE 802.15.4/Zigbee permite três tipos de topologias de rede: estrela, *mesh* e *cluster-tree* (Figura 3.15) [28].
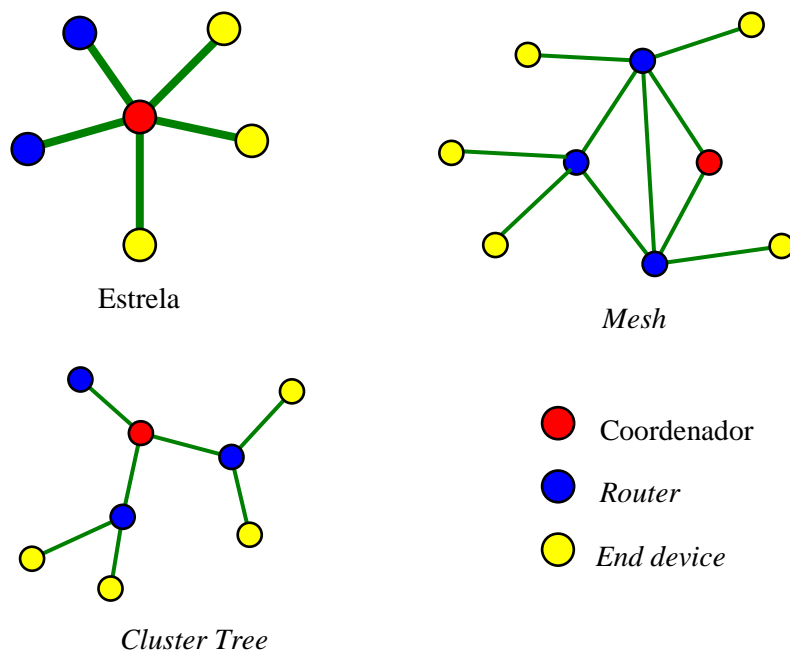
Figura 3.15 - Topologias de rede suportadas pelo IEEE 802.15.4/Zigbee

Estrela

Numa topologia em estrela a rede é controlada por um único componente, o coordenador, que é responsável pela inicialização e pela manutenção da rede. Nesta topologia, a comunicação é centralizada, uma vez que todos os outros componentes, os *end devices*, se pretendem comunicar com outro *end device*, devem enviar a mensagem ao coordenador, que por sua vez a envia ao destinatário. Esta topologia não é muito eficiente em termos energéticos, pois o coordenador consome os seus recursos energéticos rapidamente.

Mesh

A topologia *mesh* inclui um coordenador, que é responsável pela inicialização e pela identificação de toda a rede, no entanto, ao contrário da anterior, nesta topologia a comunicação é descentralizada, isto é, cada nó pode comunicar directamente com qualquer outro nó da rede, desde que esteja dentro da sua área de rádio (*ad-hoc*). Esta topologia permite assim uma maior flexibilidade, mas introduz uma complexidade adicional ao descentralizar a comunicação. Em comparação com a topologia em estrela, esta é mais eficiente ao nível energético, uma vez que o processo de comunicação não depende de um nó em particular.

Cluster-tree

A topologia *cluster-tree* é um caso especial da rede *mesh*, no qual existe apenas um caminho possível entre qualquer par de nós. Existe apenas um coordenador, que identifica toda a rede, e um *router* por cluster. Nestas redes as mensagens são encaminhadas através da rede com recurso a uma estratégia de encaminhamento hierárquica: o *end device* envia a mensagem ao *router* a que está associado, sendo depois encaminhada através dos vários *router*s até ao destino.

Todos os componentes têm atribuído pela Zigbee Alliance um endereço único IEEE de 64 *bits*, no entanto, o coordenador de uma PAN pode atribuir um endereço reduzido de 16 *bits* a cada componente dessa rede, que será único nessa PAN.

Arquitectura

A arquitectura da *stack* IEEE 802.15.4/Zigbee é constituída por um conjunto de níveis baseado no modelo OSI (Figura 3.16) [27]. Cada camada desempenha um conjunto

específico de serviços à camada imediatamente acima. As diferentes camadas comunicam entre si através de SAPs (Service Access Points), que têm dois tipos de entidades: A DE (Data Entity), que fornece o serviço de transmissão de dados, e a ME (Management Entity), que fornece todos os serviços de gestão entre os diferentes níveis.
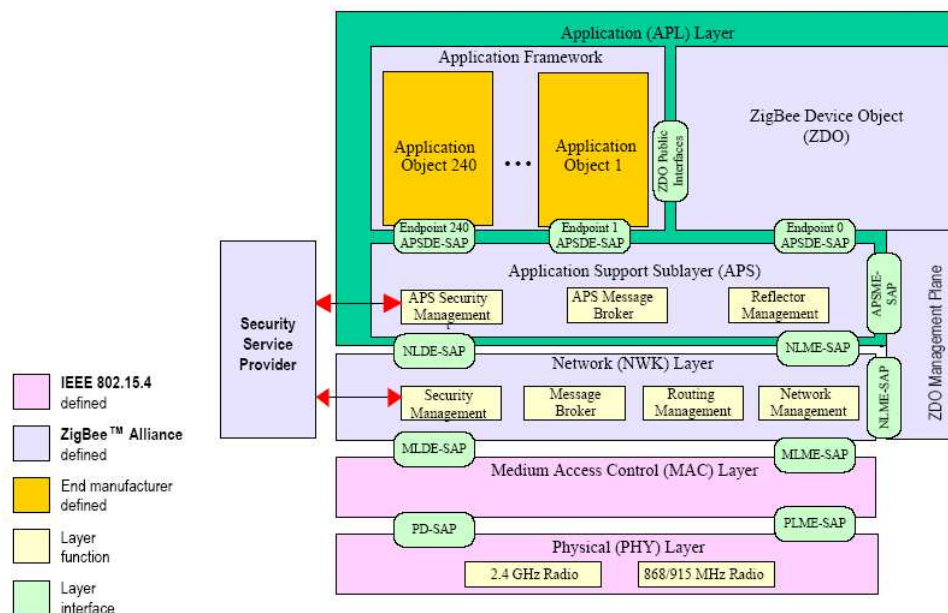
Figura 3.16 - **Arquitectura da *stack* do protocolo IEEE 802.15.4/Zigbee**

Camada Física

O IEEE 802.15.4 define duas camadas físicas que operam em bandas de frequências não licenciadas: a banda ISM de 2,4 GHz (2400 - 2483,5 MHz) a nível mundial e ainda a banda de 868 MHz (868 - 868,6 MHz) na Europa e a de 915 MHz (902 – 928 MHz) na América do Norte (figura 3.17) [22].
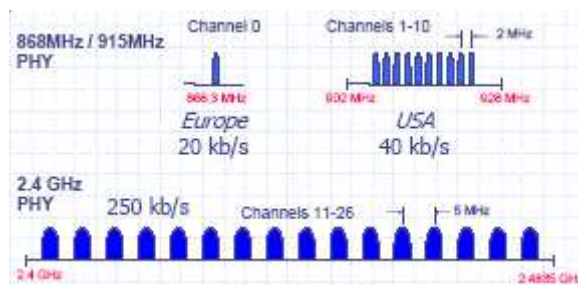
Figura 3.17 - **Bandas de frequência definidas no IEEE 802.15.4/Zigbee**

A técnica de modulação utilizada é o DSSS. Também é utilizada a FDMA, que é uma técnica que divide a largura de banda disponível em vários canais. Na banda de 2,4

GHz a taxa máxima de *bits* transmitidos por canal é de 250 Kbps, sendo que, no total, esta banda acomoda 16 canais. Na banda de 868 MHz está disponível um canal único de 20 Kbps, enquanto a banda de 915 MHz acomoda 10 canais de 40 Kbps.

Na prática, devido aos vários parâmetros dos sistemas, em especial o protocolo MAC utilizado, a taxa máxima é cerca de metade do seu valor nominal. Se os níveis superiores detectarem uma degradação da taxa de transmissão ao utilizar um canal específico dentro da largura de banda, o sistema pode procurar um canal que assegure uma melhor *performance* (excepto se transmitir nos 868 MHz, onde apenas existe um canal).

A camada física é responsável pelas seguintes tarefas: activação e desactivação do *transceiver* de rádio, detecção de energia, indicação da qualidade da transmissão, CCA (Clear Channel Assessment) e selecção do canal de frequência.

A activação e desactivação do *transceiver* de rádio é uma função da camada física. O *transceiver* pode operar num de três modos: transmissão, recepção, ou *sleep*.

A detecção de energia consiste uma estimação da potência do sinal recebido, sem identificação ou descodificação do mesmo. Esta medição é tipicamente utilizada pela camada física para verificar se o canal está *idle* ou ocupado, no processo de acesso ao meio, e também pela camada de rede, no algoritmo de escolha do canal.

A indicação da qualidade da transmissão é uma medição da qualidade do sinal recebido. Pode ser implementada através da detecção de energia, recorrendo à estimação de ruído de um sinal, ou ainda combinando as duas técnicas.

O CCA é uma avaliação da actividade do canal e opera em três modos:

Detecção de energia: O CCA indica que o meio está ocupado se detecta um sinal com um nível de energia superior ao valor limite.

Carrier Sense: O CCA indica que o meio está ocupado se detecta um sinal com as características de modulação e de *spreading* do IEEE 802.15.4.

Carrier Sense com detecção de energia: é uma combinação das duas técnicas anteriores. O CCA indica que o meio está ocupado se detecta um sinal com as características de modulação do IEEE 802.15.4 e com um nível de energia superior ao valor limite.

A selecção do canal de frequência é da responsabilidade da camada física. É esta camada que pode sintonizar o *transceiver* para um canal específico, quando tal é requisitado por uma camada superior.

Sub-camada MAC

O protocolo MAC utilizado por esta norma suporta dois modos possíveis de operação: o modo *unbeaconed* e o modo *beaconed* (figura 3.18).
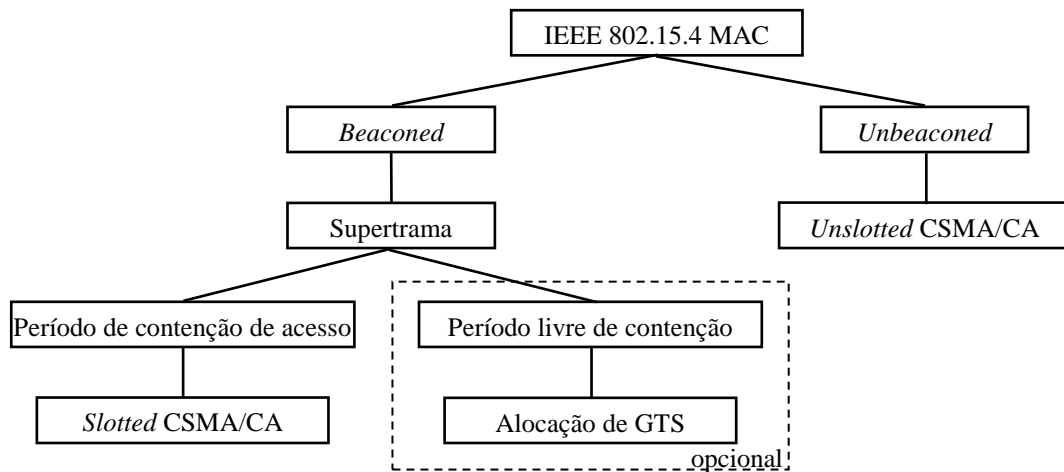
Figura 3.18 - Modos de operação do protocolo MAC no IEEE 802.15.4/Zigbee

No modo *unbeaconed* todos os componentes da rede utilizam um mecanismo de acesso ao meio do tipo CSMA/CA *unslotted*: o componente que inicia a transmissão de um pacote de dados, em vez de proceder imediatamente ao *carrier sensing*, introduz um tempo de espera aleatório (*backoff time*). Ora este *backoff time* permite que sejam evitadas colisões.

No modo *beaconed* o coordenador da rede transmite *beacons* periodicamente, para sincronizar os nós a ele associados, bem como para identificar a PAN. Os *beacons* indicam o início de uma estrutura do tipo supertrama (Figura 3.19).
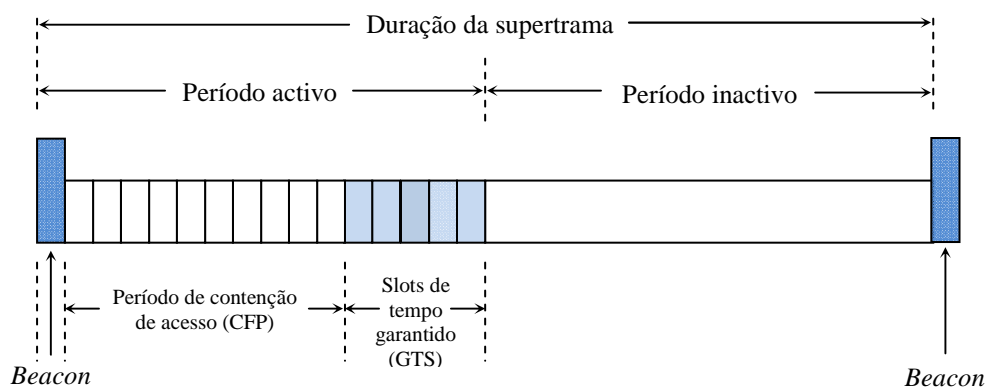
Figura 3.19 - Estrutura da supertrama no modo *beaconed* do Zigbee

A supertrama consiste num período activo e num período inactivo.

O período activo está dividido em 16 *slots* de tempo e é composto pelo próprio beacon, pelo período de contenção de acesso e pelo período de contenção opcional.

O beacon é transmitido no início do *slot* 0 e contém informação acerca dos campos de endereçamento, da especificação da supertrama e dos campos de GTS.

O período de contenção de acesso inicia imediatamente a seguir ao beacon e durante este período o acesso ao meio é realizado através de um mecanismo do tipo CSMA/CA *slotted*.

A seguir pode ocorrer um período livre de contenção, opcional, durante o qual o coordenador da rede aloca *slots* de tempo garantido (GTS – *Guaranteed Time Slots*) aos RFDs que necessitem de uma largura de banda garantida para a transmissão de dados.

No fim da supertrama existe um período inactivo, durante o qual todos os nós, incluindo o coordenador, podem entrar em *stand-by* para poupar energia.

Formato geral de uma trama da camada MAC

O standard IEEE 802.15.4 define quatro tipos de tramas: as tramas de *beacon*, de dados, de comandos e de *acknowledgment*. O formato geral de uma trama especificada por este *standard* está ilustrado na figura 3.20 [30].
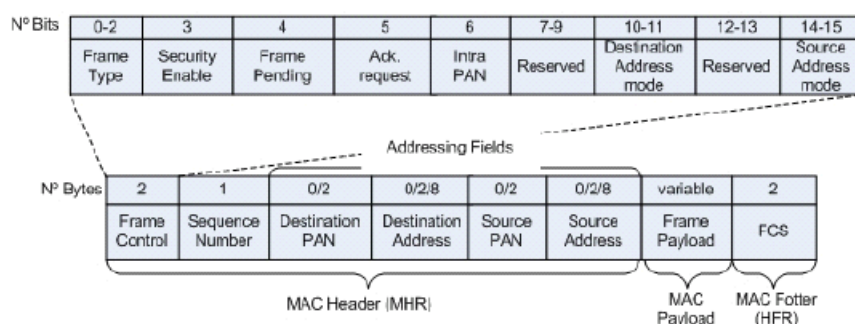
Figura 3.20 - Formato geral de uma trama da sub-camada MAC IEEE 802.15.4

Uma trama IEEE 802.15.4 é composta pelo *header*, pelo *payload* e pelo *fotter*. O *header* é constituído pela trama de controlo, pelo campo do número sequencial e pelos campos de encaminhamento.

Os campos da trama de controlo têm uma ordem fixa e são os seguintes:

Tipo de trama – dados, *beacon*, comando ou *acknowledge*;

Segurança – indica se a trama está encriptada;

Pending – indica se existe alguma informação pendente (no caso de o componente

destino ter requisitado informação ao coordenador, se a informação for extensa pode ser enviada em várias tramas);

Acknowledge request – indica pedido de *acknowledge*;

Intra PAN – se a transmissão for dentro da PAN, não há necessidade de identificar a PAN de destino;

Tipo de Endereço do destino – indica o tipo de endereço presente nos campos de endereçamento (endereço reduzido de 16 *bits* ou endereço IEEE 64 *bits*);

Tipo de Endereço da fonte – indica o tipo de endereço presente nos campos de endereçamento (endereço reduzido de 16 *bits* ou endereço IEEE 64 *bits*);

Os campos de endereçamento incluem a seguinte informação:

Número sequencial – campo de oito *bits* que define um número sequencial único que identifica a trama;

Identificador da PAN destino – se presente, define o endereço reduzido de 16 *bits* da PAN fonte;

Endereço do componente destino – se presente, define o endereço reduzido de 16 *bits* ou o endereço IEEE de 64 *bits* do componente destino;

Identificador da PAN fonte – se presente, define o endereço reduzido de 16 *bits* da PAN fonte;

Endereço do componente fonte – se presente, define o endereço reduzido de 16 *bits* ou o endereço IEEE de 64 *bits* do componente fonte;

Camada de rede

A camada de rede é responsável pelos procedimentos de gestão da rede, tais como: inicialização de rede, associação e desassociação de nós, endereçamento, configuração dos componentes da rede, formação e manutenção do NIB (Network Information Base), encaminhamento de mensagens e ainda outros serviços relacionados com a segurança da rede.

A camada de rede suporta duas entidades de serviços: a NLDE (Network Layer Data Entity) e a NLME (Network Layer Management Entity).

A NDLE fornece os serviços transmissão de dados que permitem o transporte de NPDUs (*Network Application Protocol Data Units*) entre dois ou mais componentes da mesma rede, que são:

Geração do NPDU – é da responsabilidade da NDLE a geração de PDUs da camada

de rede;

Encaminhamento – a NDLE tem de proceder ao encaminhamento dos NPDUs, específico da topologia da rede em que o componente está inserido;

Segurança – a NDLE deve ter a capacidade de assegurar, não só a autenticidade, como a confidencialidade da transmissão.

A NLME fornece os serviços de gestão que permitem que uma aplicação interaja com a *stack* do protocolo Zigbee. Esses serviços são:

Configuração de um novo componente – inclui iniciar a operação como coordenador, ou integrar uma rede existente;

Inicialização de uma rede – um componente com funções de coordenador tem a capacidade de inicializar uma rede

Associação, reassociação e desassociação de uma rede – qualquer componente pode pedir para se associar, reassociar ou desassociar de uma rede e qualquer coordenador ou *router* deve ter a capacidade de pedir a um componente para proceder a qualquer uma das três acções;

Endereçamento – os coordenadores e os *router*s devem ter a capacidade de atribuir endereços reduzidos de 16 *bits* aos componentes que integram a rede;

Descoberta de componentes vizinhos – a NLME deve ter a capacidade de descobrir, guardar e relatar informação relativa aos vizinhos de um salto do componente;

Descoberta de um caminho - a NLME deve ter a capacidade de descobrir e guardar caminhos através da rede, contribuindo para um encaminhamento eficaz de mensagens;

Controlo de recepção – qualquer componente deve ter a capacidade de controlar quando e por quanto tempo a recepção de mensagens é activada, permitindo assim o sincronismo da sub-camada MAC;

Encaminhamento – a NLME deve ter a capacidade de utilizar diferentes mecanismos de encaminhamento (*unicast*, *broadcast*, *multicast* ou muitos para um) tendo como objectivo final uma troca de dados eficiente dentro da rede.

Formato geral de uma trama da camada de rede

O standard Zigbee define dois tipos de tramas: as tramas de dados e as tramas de comandos.

O formato geral de uma trama Zigbee do nível de rede está ilustrado na figura 3.21 [30].
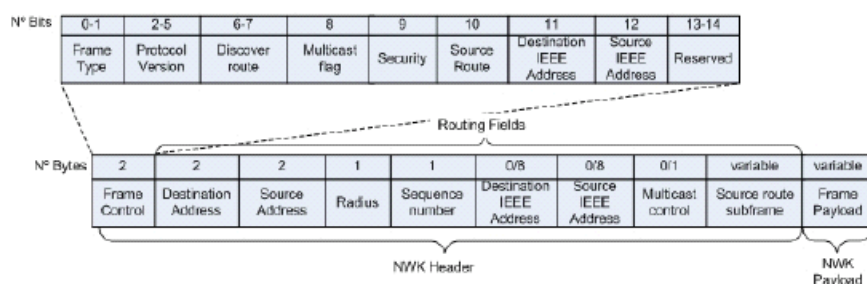
Figura 3.21 - Formato geral de uma trama do nível de rede Zigbee

Uma trama Zigbee é composta pelo header e pelo *payload*.

O *header* é constituído pela trama de controlo e pelos campos de encaminhamento.

A trama de controlo inclui os seguintes campos:

Tipo de trama – 0 se é uma trama de dados, 1 se é de comando;

Versão do protocolo – verão do protocolo Zigbee utilizada;

Descoberta de caminho – indica a opção escolhida acerca da descoberta de caminho: 0x00 se inibe a descoberta de caminho, 0x01 se permite a descoberta de caminho, 0x02 se força a descoberta de caminho;

Campo *multicast* – é 1 se se trata de uma trama *multicast*, é 0 se for uma trama do tipo *unicast* ou *broadcast*;

Segurança – é 1 se os procedimentos de segurança estiverem activados;

Endereço IEEE do destino – indica a presença do endereço de 64 *bits* do destino nos campos de encaminhamento;

Endereço IEEE da fonte – indica a presença do endereço de 64 *bits* da fonte nos campos de encaminhamento;

Os campos de encaminhamento incluem a seguinte informação:

Endereço reduzido do destino – endereço de 16 *bits* do destino;

Endereço reduzido da fonte – endereço de 16 *bits* da fonte;

RADIUS – alcance da transmissão de rádio. Este valor é decrementado em uma unidade por cada *relay*, se atingir o zero a trama é descartada;

Campo de número sequencial – número sequencial único que identifica a trama;

Endereço IEEE do destino – endereço de 64 *bits* do destino;

Endereço IEEE da fonte – endereço de 64 *bits* da fonte;

Controlo *multicast* – parâmetros de controlo de fluxo de transmissão *multicast*;

Subtrama do caminho fonte – este campo inclui uma lista de endereços *relay*, que

contém os seguintes campos: número de nós *relay* incluídos na lista, próximo relay e endereços reduzidos dos nós *relay*.

Camada de aplicação

A camada de aplicação é a camada superior e inclui: a sub-camada APS (Application Support Sub-layer), a AF (Application Framework) e o ZDO (Zigbee Device Object).

APS

A APS fornece a *interface* entre a camada de rede e a camada de aplicação, através de um conjunto de serviços que podem ser utilizados, tanto pelo ZDO, como pelos objectos de aplicação específicos do fabricante e incluídos na AF. Esses serviços são fornecidos através de duas entidades: o APSDE (APS Data Entity) e o APSME (APS Management Entity).

O APSDE fornece serviços de transmissão de dados através do SAP a ele associado, o APSME-SAP, entre duas ou mais entidades de aplicação localizadas na mesma rede. Os serviços fornecidos são os seguintes:

Geração do APDU – o APSDE deve ser capaz de pegar num APDU e gerar um APS-PDU, acrescentando o *overhead* apropriado;

Binding – depois de concluído o *binding* entre dois componentes, o APSDE deve ser capaz de transferir mensagens de um componente para outro;

Filtro de endereço de grupo – é a capacidade de filtrar mensagens endereçadas a um grupo de componentes;

Transporte fiável – aumenta a fiabilidade das transacções relativamente ao nível de rede, ao utilizar *retries*;

Rejeição de duplicados – as mensagens transmitidas são recebidas apenas uma vez;

Fragmentação – permite a segmentação e o *reassembly* de mensagens maiores que o *payload* de uma trama do nível de rede.

O APSME fornece serviços de gestão a objectos de aplicação através do SAP a ele associado, o APSME-SAP, e mantém uma base de dados dos objectos geridos, a AIB (APS Information Base). Os serviços fornecidos são:

Gestão de *binding* – é o estabelecimento de uma ligação entre dois componentes de uma rede;

Gestão de AIB – introduzir ou retirar atributos da AIB;

Segurança – é a capacidade de estabelecer autênticas relações com outros

componentes, com recurso a chaves de segurança;

Gestão de grupo – é a funcionalidade de declarar um endereço de grupo partilhado por múltiplos componentes, bem como de adicionar ou remover componentes desse grupo.

AF

O AF é o ambiente onde se encontram os objectos de aplicação nos componentes Zigbee. Podem ser definidos até 240 objectos de aplicação distintos, sendo cada um identificado por um endereço de *endpoint* entre 1 e 240. São definidos dois *endpoints* adicionais para utilização do APSDE-SAP: o *endpoint* 0 é reservado para a *interface* de dados do ZDO e o *endpoint* 255 é reservado para a *interface* de dados no *broadcast* de dados para todos os objectos de aplicação. Os *endpoints* 214 a 254 estão reservados para utilizações futuras.

Os objectos de aplicação são aplicações específicas do próprio fabricante, que correm em cima da *stack* Zigbee. Cada objecto de aplicação satisfaz um determinado perfil aprovado pela Zigbee Alliance. Um exemplo de um perfil Zigbee é a *home automation*. Este perfil Zigbee permite que uma série de componentes troquem mensagens de controlo, com vista a formar uma aplicação sem fios de *home automation*. Estes componentes são designados para trocar mensagens cujo efeito será, por exemplo, o ON/OFF de um ponto de luz, o envio de uma medição de um sensor de luz a um controlador de luminosidade, ou o envio de uma mensagem de alerta caso um sensor de ocupação detecte movimento.

Actualmente os perfis Zigbee disponíveis abrangem as seguintes áreas: gestão de energia e eficiência energética, automação de casas, automação de edifícios e controlo industrial.

ZDO

O ZDO inclui um conjunto de aplicações que utilizam primitivas da camada de rede e da APS para implementar os componentes Zigbee: coordenadores, *router*s e *end device*s. O ZDO é responsável pelas seguintes operações:

Inicialização do APS, da camada de rede e do SSP (*Security Service Provider*);

Reunião da informação de configuração das aplicações finais, para determinar e implementar a descoberta de novos componentes, a gestão de procedimentos de segurança, a gestão da rede e a gestão de *bindings*.

A *interface* do ZDO com a APS é realizada no *endpoint* 0, através do APSDE-SAP para dados e através do APSME-SAP para mensagens de controlo.

3.4.4 Coexistência de tecnologias sem fios

Tem sido objecto de estudo a utilização de várias tecnologias sem fios num único ambiente. Tal não é problema, desde que as diferentes tecnologias funcionem em larguras de banda diferentes. Tal como indicado anteriormente, a banda dos 2,4 GHz está atribuída ao Bluetooth, ao Zigbee, ao Wi-Fi e possivelmente a outros sistemas. Torna-se então necessário investigar o desempenho dos sistemas coexistentes e introduzir métodos para a redução de problemas entre eles.

O CSMA é um mecanismo que melhora a coexistência de múltiplos sistemas de comunicação que utilizam a mesma largura de banda. De facto, o objectivo de uma operação do tipo *carrier-sensing* é evitar interferir com transmissões que já estão a decorrer. No entanto, depende da implementação do mecanismo de *carrier-sensing* se transmissões de outros tipos de sistemas sem fios podem ser detectadas ou não.

No IEEE 802.15.4, por exemplo, o utilizador pode escolher entre diferentes modos de *carrier-sensing*. Num modo, o circuito do *carrier-sensing* indica um meio ocupado quando a energia do sinal recebido é maior que um determinado valor pré-estabelecido, não interessando se o sinal vem de qualquer outro sistema que actue naquela largura de banda. Noutro modo é requerido que o sinal recebido seja correctamente descodificado, isto é, seja utilizado o esquema de modulação correcto. Neste modo, uma estação IEEE 802.15.4 apenas pode detectar transmissões a decorrer emitidas por outras estações IEEE 802.15.4 e nunca de estações com outro protocolo.

A interferência entre o Bluetooth e o IEEE 802.11b tem sido objecto de extensivas investigações [21]. É pelo menos o caso dos sistemas com frequência estática, como o IEEE 802.11. Quando múltiplos sistemas Bluetooth AFH-*enabled* operam em paralelo com uma rede IEEE 802.11, todos os sistemas Bluetooth deixam de operar nos canais ocupados pela rede IEEE 802.11, tendo de partilhar entre si os restantes canais. Como passam a haver menos canais disponíveis para os sistemas Bluetooth, estes provocam mais interferência entre si. Juntamente com a introdução do AFH, foi feita outra melhoria na versão 1.2 do Bluetooth, relativamente à coexistência entre sistemas, nas versões anteriores o pacote de *reverse link* que contém o *acknowledgement* era transmitido numa frequência diferente da do pacote de *forward link*. Assim, a probabilidade de perdas aumentava, caso existisse uma interferência estática, uma vez que o *reverse link* podia saltar para a banda com interferência, mesmo que a transmissão *forward link* fosse bem sucedida. Na versão 1.2 ambos os pacotes são transmitidos na mesma frequência, logo não é possível ocorrer tal

situação. Se um sistema Bluetooth e um IEEE 802.11b actuam tão próximos que a potência de transmissão do IEEE 802.11b bloqueia os receptores Bluetooth de receberem transmissões então, desde que as antenas estejam separadas menos 20 a 30 cm, pode-se recorrer a métodos como um *joint scheduler* para permitir a coexistência entre os dois sistemas.

Por sua vez, também têm sido realizados estudos para verificar a coexistência de sistemas Zigbee e Wi-Fi. Uma vez que o IEEE 802.15.4 e o IEEE 802.11b são de frequência estática, e podendo essa frequência ser alterada manual ou automaticamente, em [21] foi concluído que o IEEE 802.15.4 tem pouco ou nenhum impacto no IEEE 802.11b, desde que seja feita uma gestão cuidada das frequências. Além disso, é esperado que as aplicações típicas do IEEE 802.15.4 tenham um *duty cycle* baixo, entre 0.1 e 1 %, o que significa que as estações não transmitem durante 99.9 a 99 % do seu tempo, respectivamente. Ora as estações que operam com este *duty cycle* não podem criar uma interferência significativa na comunicação de outras redes.

3.4.5 Comparação entre sistemas sem fios

Neste capítulo foram estudados três sistemas sem fios. Todos eles foram concebidos para a utilização em diferentes cenários, apresentando várias vantagens e desvantagens, dependendo da sua utilização. Na escolha de um protocolo para o desenvolvimento de uma aplicação deve-se optar pelo protocolo que melhor se adequa às exigências requeridas pela própria aplicação, tendo em conta o tipo de aplicação, a distância de comunicação necessária e a taxa de transferência pretendida.

A figura 3.22 indica a área de trabalho dos actuais standards sem fios da família IEEE 802, tendo em conta o tipo de dados a transmitir e o tamanho da rede [29].
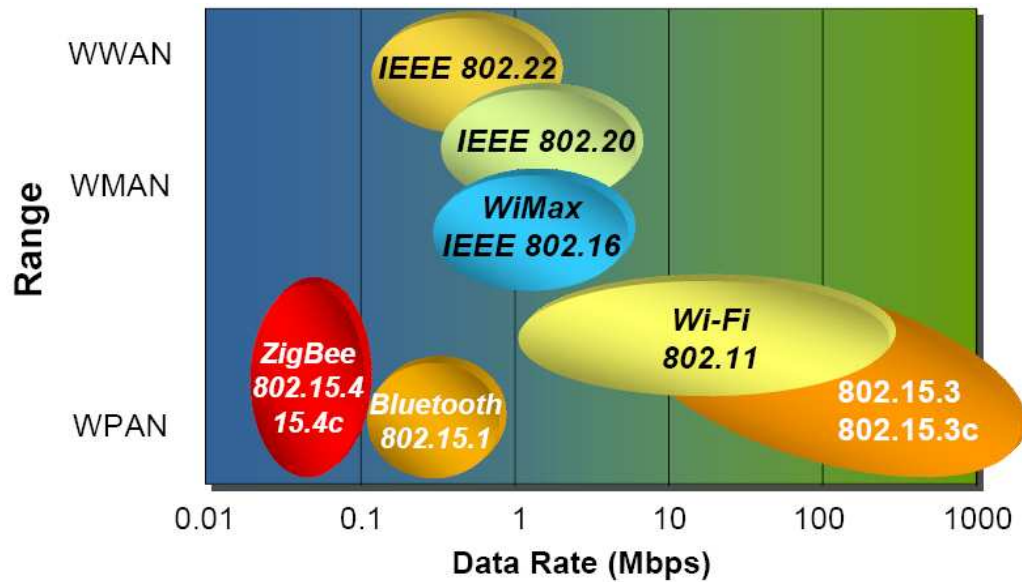
Figura 3.22 - **Áreas de aplicação dos *standards* da família IEEE 802**

Os sistemas IEEE 802.11/Wi-Fi são indicados para a transmissão de grandes quantidades de dados. O IEEE 802.15.4/Zigbee é aconselhado para comunicações pouco frequentes, com pequenos pacotes de dados e quando o consumo de energia deve ser baixo. O IEEE 802.15.1/Bluetooth preenche o vazio entre estes dois protocolos, sendo adequado para a transmissão de dados de tamanho médio e com baixo consumo de energia (Tabela 3.2) [29].

Tabela 3.2 - Comparação entre as tecnologias sem fios analisadas

	IEEE 802.11/Wi-Fi	IEEE 802.15.1/Bluetooth	IEEE 802.15.4/ Zigbee
Tipo de aplicação	Internet dentro de edifícios	Periféricos de computadores e de telemóveis	Monitorização e controlo
Alcance (m)	100 m	10 m	100 m
Tamanho da rede (nº de componentes)	32	7	2^{64}
Topologia	Estrela	Estrela	Estrela, *tree*, *cluster-tree*
Consumo de energia	Médio	Baixo	Muito baixo
Frequência	2,4 GHz	2,4 GHz	2,4 GHz, 868/915 MHz
Nº. de canais	11-14	78	16 – 2,4 GHz 1 – 868 KHz 10 – 915 KHz
Taxa de transmissão de dados máxima	11 Mbps	1 Mbps	250 Kbps – 2,4 GHz 20 Kbps – 868 KHz 40 Kbps – 915 KHz
Características	Velocidade de transmissão de dados, flexibilidade	Baixo custo	Fiabilidade, baixo consumo de energia, baixo custo

Apesar de qualquer um dos sistemas poder ser utilizado no chão de fábrica, nenhum deles poderá operar nos seus níveis normais de *performance*, devido às condições adversas para a transmissão via rádio existentes nesses ambientes, tais como a interferência ou o *frequency-selective fading*, que são particularmente prevalecentes em sistemas que operam na banda ISM de 2,4 GHz [21].

Pelas suas características, o IEEE/Zigbee apresenta-se como uma alternativa interessante para o tipo de comunicação existente no chão de fábrica. Esta tecnologia destina-se ao envio de pacotes de dados pequenos, a comunicação pode ser iniciada a pedido de qualquer elemento da rede, o que permite uma boa gestão da comunicação na rede e tem um baixo consumo de energia, podendo mesmo as estações gerir o tempo em que estão em modo de poupança de energia, o que permite uma maior eficiência energética. É, no entanto, ainda uma norma em aberto, sendo objecto de estudo, não só por parte dos fabricantes que desenvolvem soluções baseadas nesta tecnologia, mas também na

comunidade científica, com vista à melhoria da sua performance. Actualmente já existem bastantes soluções certificadas pela Zigbee Alliance, sendo de destacar as apresentadas por alguns dos fabricantes mais conhecidos: Atmel, Chipcon/Texas Instruments, Crossbow, Ember, Freescale, Jennic, Oki, Oner e Renesas (Figura 3.23) [26].

Figura 3.23 - Algumas soluções baseadas na tecnologia IEEE 802.15.4/Zigbee

a) Freescale
b) Ember
c) Oki
d) Atmel
e) Crossbow
f) Jennic
g) Chipcon/Texas Instruments
h) Oner
i) Renesas

3.5 Conclusão

Neste capítulo foram estudados alguns assuntos relacionados com as redes sem fios.

As tecnologias sem fios podem trazer muitos benefícios às aplicações industriais, sendo uma delas a possibilidade de reduzir os tempos de *setup* das máquinas, ao evitar a cablagem. O mercado já oferece soluções sem fios maturas, como o Wi-Fi, o Bluetooth ou o Zigbee. Até agora, no entanto, as tecnologias sem fios ainda não ganharam uma razoável aceitação no chão de fábrica. Uma das razões para tal facto é a dificuldade em conseguir uma transmissão em tempo real bem sucedida em canais propensos a erros. Com o desenvolvimento de mecanismos de protocolos e de esquemas de transmissão apropriados, juntamente com a cuidadosa combinação dos mesmos, poderão ser dados grandes passos no sentido de aumentar a aceitação de tecnologias sem fios em aplicações industriais.

Existem muitas oportunidades de investigação no campo das comunicações industriais sem fios, que envolvem a procura de novos mecanismos de protocolo que melhorem a *performance* em tempo real. Um componente chave no *design* e na avaliação de tais mecanismos é a formulação de medidas de *performance* apropriadas a aplicações *benchmark* e modelos de canais sem fios adaptados a ambientes industriais.

Outras áreas de investigação envolvem áreas como a segurança, o apoio à mobilidade e ainda o objectivo comum de transmissão em tempo real e eficiência energética.

4 Sistema de instrumentação distribuída suportado por rede sem fios

4.1 Introdução

As necessidades de disponibilização de informação proveniente do nível de campo (sensores e actuadores) são cada vez maiores e mais importantes. O acesso a esta informação era até há pouco tempo atrás efectuado recorrendo a tecnologias baseadas em comunicação com fio. Com o desenvolvimento das tecnologias sem fios os custos elevados e os inconvenientes associados à cablagem deixaram de existir. A disponibilização de informação através de tecnologia sem fios permite monitorizar e controlar locais e/ou situações onde até agora seria extremamente dispendioso ou até impossível colocar cablagem.

As tecnologias de comunicações sem fios surgem como uma alternativa às tradicionais arquitecturas baseadas em comunicação através de fios. A possibilidade de aceder à informação, qualquer que seja o ponto onde esta se encontre, permite progressos na instrumentação dos processos industriais.

O objectivo principal de qualquer sensor ou sistema baseado em sensores é adquirir informação, seja ela relativa a temperatura, taxa de fluxos, nível de inventário, performance da máquina, ou qualquer outro parâmetro que possa ser medido. Enquanto gerar dados a partir de sensores é directo e muito bem compreendido, o transporte dos dados desde o sensor para o sistema de monitorização ou de controlo continua a ser um desafio, devido ao custo, à complexidade da instalação e à manutenção da rede de comunicações sobre a qual está implementado o sistema.

Em muitas aplicações os sensores são implementados nos próprios sistemas que monitorizam, em grande parte devido à falta de uma solução sem fios apropriada, estável e de baixo custo. Os protocolos de comunicação sem fios, incluindo o Wi-Fi, Bluetooth e

Zigbee, emergiram em grande parte para proporcionar uma maior flexibilidade relativamente aos sistemas com fio.

As comunicações com suporte físico em fios, tais como ModBus, LonTalk, DeviceNet, CAN ou HART desempenham um excelente trabalho na integração de sensores nos seus ambientes e proporcionam tipicamente grandes níveis de confiança. As redes com fios são convenientes sempre que estiver em causa uma missão com tempos ou dados críticos e segurança elevada, no entanto a cablagem de uma instalação é extremamente cara e qualquer alteração é bastante dispendiosa e demorada, o que leva a que os sistemas baseados em comunicações com fio sejam muito rígidos nas suas arquitecturas. Mesmo que a alteração da arquitectura seja pequena implica sempre o levantamento da antiga instalação, com nova cablagem e nova disposição dos sensores que irão monitorizar o processo.

A facilidade de instalação e a flexibilidade das comunicações sem fios são os seus pontos positivos, enquanto os pontos negativos são o custo e a confiança.

Com o incremento do número de tecnologias normalizadas disponíveis no mercado, como o Wi-Fi, o Bluetooth e o Zigbee, o custo destas tecnologias caiu abruptamente. A generalização da sua utilização e os consequentes aumentos do desenvolvimento e da oferta de produtos baseados nestas tecnologias, permitiu um significativo aumento da confiança e do alcance das redes sem fios.

No entanto outra questão se coloca: Qual a melhor solução para a tecnologia sem fios a utilizar? Uma solução baseada em tecnologia proprietária ou baseada em standards?

Esta questão nem sempre tem uma resposta clara e simples. Um sistema baseado em sensores que requer a flexibilidade de uma rede sem fios pode ser implementado utilizando tecnologias proprietárias ou baseadas em standards.

Os sistemas proprietários são realizados de acordo com uma aplicação específica, podendo oferecer benefícios em termos de distância de transmissão, do consumo de energia e do custo por unidade. No entanto, na generalidade são pouco seguros e a sua natureza proprietária implica que os desenvolvimentos da indústria de massas não lhes sejam aplicados. As grandes desvantagens destes sistemas são: a complexidade, o risco de uma solução proprietária, bem como a dependência de um fabricante.

Os sistemas baseados em tecnologias standards têm grandes vantagens, sendo de destacar as seguintes: a utilização de uma tecnologia do domínio público, o desenvolvimento e produção em grandes quantidades, a inerente diminuição dos custos do

projecto e da sua implementação, o aumento da oferta por parte dos fabricantes e a consequente concorrência, com a respectiva diminuição dos preços.

A escolha da tecnologia a utilizar no desenvolvimento de um sistema de instrumentação deve ser bem ponderada. Para tal devem ser analisados todos os requisitos do sistema e a arquitectura que se pretende implementar no desenvolvimento do sistema de instrumentação.

4.2 Requisitos do sistema de instrumentação distribuída

Antes de iniciar qualquer apresentação sobre os requisitos a implementar no Sistema de Instrumentação Distribuída, é necessário definir o sistema que se pretende implementar e quais as funções que o mesmo deve desempenhar.

O Sistema de Instrumentação Distribuída pode ser definido como um sistema onde decorrem aplicações de aquisição de sinal proveniente de sensores implementados, por exemplo, num ambiente industrial, com a possibilidade de armazenamento e processamento da informação, bem como o seu posterior envio para níveis superiores.

A denominação de "Sistema de Instrumentação Distribuída Suportado por Rede sem Fios" pretende não só realçar o facto de este tipo de equipamento permitir uma mobilidade na arquitectura do sistema de aquisição de sinal, mas também a possibilidade de acesso por parte de terceiros a toda a informação proveniente do sistema de uma forma simples e eficiente, sem a necessidade de cablagem associada.

Em termos de aplicação prática o Sistema de Instrumentação Distribuída pode ser decomposto em duas partes: o *hardware* e o *software*.

O *hardware* compreende a interligação de todos os dispositivos que fazem parte do sistema, que são: os nós que incluem os sensores, o sistema de aquisição de dados e o sistema de tratamento e envio de dados através de comunicação sem fios.

O *software* inclui o controlo e a integração de todos os dispositivos de *hardware*. As suas principais funções são a aquisição de dados e a comunicação sem fios entre os vários elementos que compõem o Sistema de Instrumentação Distribuída e ainda a comunicação com fios entre o colector de dados e um PC.

Os requisitos propostos para o Sistema de Instrumentação Distribuída são:

- O custo do *hardware* associado a cada nó deve ser baixo, pois uma grande parte do custo total do sistema está associado a esta parcela. Para que o sistema seja uma

alternativa aos produtos existentes actualmente no mercado, o preço é um factor fundamental no seu sucesso.

- A solução a adoptar deve permitir a ligação de vários tipos de sensores ao mesmo módulo de aquisição de sinal. Desta forma podem ser monitorizadas várias grandezas, sendo fácil a implementação de uma rede de sensores para análise de um determinado processo.
- A comunicação com o módulo central, o nó de instrumentação, deve ser clara e simples, permitindo a ligação de vários módulos sensores ao nó.
- Devem poder ser monitorizados vários elementos ao mesmo tempo, a partir da mesma unidade central.
- O *software* de comunicações não deve ter quaisquer problemas com tempos de resposta, de modo a ser compatível com a monitorização de processos que exijam respostas em tempo real, como é o caso dos processos industriais.
- O *software* de comunicações deve ser de dimensões reduzidas para poder ser implementado em plataforma com recursos reduzidos de memória.
- A possibilidade de alimentação a partir de baterias é um ponto determinante. É bastante interessante possuir um sistema de monitorização sem fios, independente da alimentação da rede, tendo-se desta forma um sistema totalmente independente de fios, quer para comunicação, quer para alimentação.
- A integração do sistema de instrumentação distribuída na arquitectura do processo a monitorizar deve ser clara e o mais simples possível, para evitar quaisquer conflitos com outro *hardware* ou *software* instalado. Após a instalação estar concluída deve ser totalmente independente de qualquer intervenção de um operador.

Com base na definição dos requisitos, é em seguida apresentada uma proposta para a arquitectura a implementar na construção do sistema de instrumentação distribuída suportado por rede sem fios.

4.3 Proposta para a arquitectura do sistema de instrumentação distribuída

Após a descrição dos requisitos para a realização do sistema de instrumentação distribuída, o passo seguinte consiste na apresentação da arquitectura a utilizar.

O sistema de instrumentação distribuída engloba os seguintes componentes: os sensores e o nó de instrumentação, que comunicam entre si recorrendo a uma tecnologia sem fios. O nó de instrumentação comunica com o PC através de uma tecnologia com fios (figura 4.1).
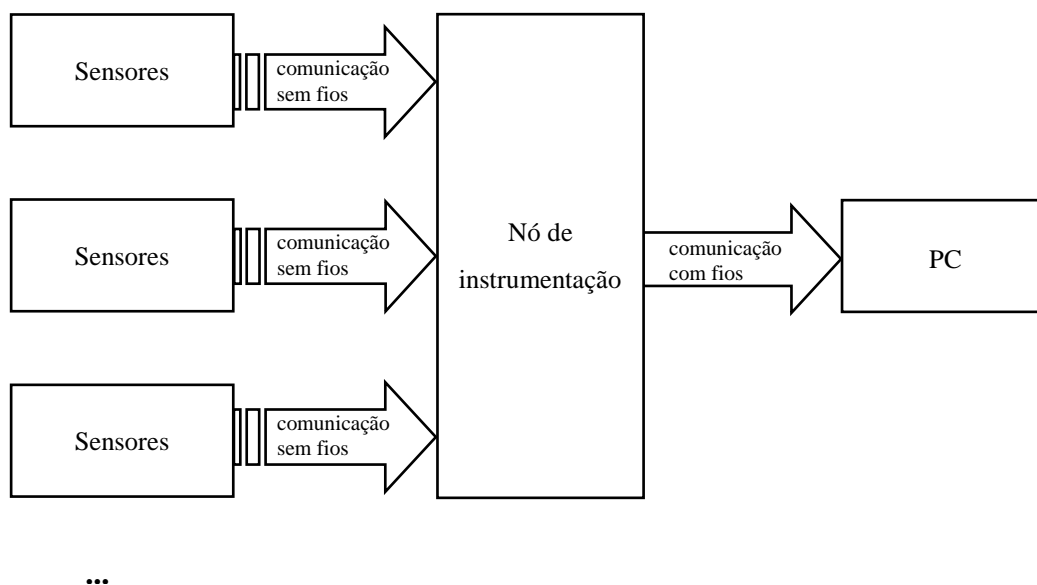
Figura 4.1 - Proposta para a arquitectura do sistema de instrumentação distribuída

4.3.1 Arquitectura do *hardware*

Tendo em conta os requisitos definidos, e após uma procura no mercado sobre as soluções existentes que utilizam tecnologia sem fios, a decisão sobre o *hardware* recaiu sobre um dispositivo que implementa o protocolo IEEE 802.15.4/Zigbee, o CC2431 da Chipcon/Texas Instruments.

As principais razões para a escolha desta plataforma são:

- O protocolo IEEE 802.15.4/Zigbee é adequado para sistemas deste tipo, onde se pretende a transmissão de pequenos pacotes de dados;
- O CC2431 inclui um sensor interno de temperatura e um monitor de bateria;
- Tem um baixo consumo de corrente: 27 mA com o microcontrolador a trabalhar a uma frequência de 32 MHz, 0,5 µA no modo *power-down* e 0,3 µA no modo *stand-by*. Este é um factor importante, uma vez que se pretende um sistema sem fios, devendo o consumo ser o mais baixo possível de forma a assegurar um longo tempo de vida das baterias que alimentam as placas onde os sensores estarão implementados.
- Inclui um conversor AD com uma resolução de 12 bits e 8 canais de aquisição de

dados, necessário para a aquisição de dados obtidos através de sensores externos. Assim, não é necessário recorrer a uma segunda placa para a aquisição de dados, o que, não só é importante no que toca ao custo do sistema, mas fundamentalmente permite ter módulos sensores de dimensões mais reduzidas;

- Permite comunicação USB e RS232 com outros dispositivos. Estas funcionalidades são importantes para a comunicação entre o sistema de aquisição de dados e um PC;
- A fiabilidade e a universalidade do próprio fabricante, a Chipcon/Texas Instruments.

4.3.2 Arquitectura do *software*

A plataforma de *software* engloba os seguintes componentes:

- Nos módulos sensores engloba a aquisição dos sinais provenientes dos sensores e a comunicação sem fios entre estes módulos e o nó de instrumentação;
- no nó de instrumentação engloba a comunicação sem fios, a aquisição e o tratamento dos dados provenientes dos módulos sensores e a comunicação com fios entre este nó e o PC.

4.4 Aspectos da implementação do sistema de instrumentação

O Sistema de instrumentação é composto por duas plataformas: uma plataforma de *hardware* e uma plataforma de *software*.

O *hardware* é constituído por duas partes:

- os módulos sensores, onde é efectuada a aquisição de sinal através de sensores (internos e externos à placa CC2431) e
- o nó de instrumentação, onde são reunidos os dados provenientes dos vários módulos sensores.

Quanto ao *software*, devido às funções distintas desempenhadas por cada elemento do *hardware*, torna-se necessário distinguir o *software* implementado nos módulos sensores do implementado no nó de instrumentação.

Nos módulos sensores será implementado o seguinte *software*:

- Aquisição de sinal: configuração do *hardware* de aquisição de sinal e respectiva

aquisição de sinal a partir dos sensores (internos e externos à placa CC2431);

- Comunicação IEEE 802.15.4/Zigbee: a aplicação de comunicação sem fios entre os módulos sensores e o nó de instrumentação é baseada na Z-stack da Chipcon/Texas Instruments;

No nó de instrumentação será implementado o seguinte *software*:

- Comunicação IEEE 802.15.4/Zigbee: a aplicação de comunicação sem fios entre o nó de instrumentação e os módulos sensores é baseada na Z-stack da Chipcon/Texas Instruments;
- Aquisição e tratamento dos dados provenientes dos módulos sensores para posterior envio dos mesmos para o PC;
- Comunicação RS232: o nó de instrumentação comunica com o PC através do protocolo RS232.

Estas plataformas serão exploradas nas secções seguintes.

4.4.1 Plataforma de *hardware*

A plataforma de *hardware* encontra-se dividida em duas partes (Figura 4.2):

- Aquisição de sinal e comunicação IEEE 802.15.4/Zigbee nos SOC-BB (System On Chip – Battery Board);
- Comunicação IEEE 802.15.4/Zigbee, recolha de dados dos elementos monitorizados e comunicação série RS232 no SmartRF Evaluation Board.
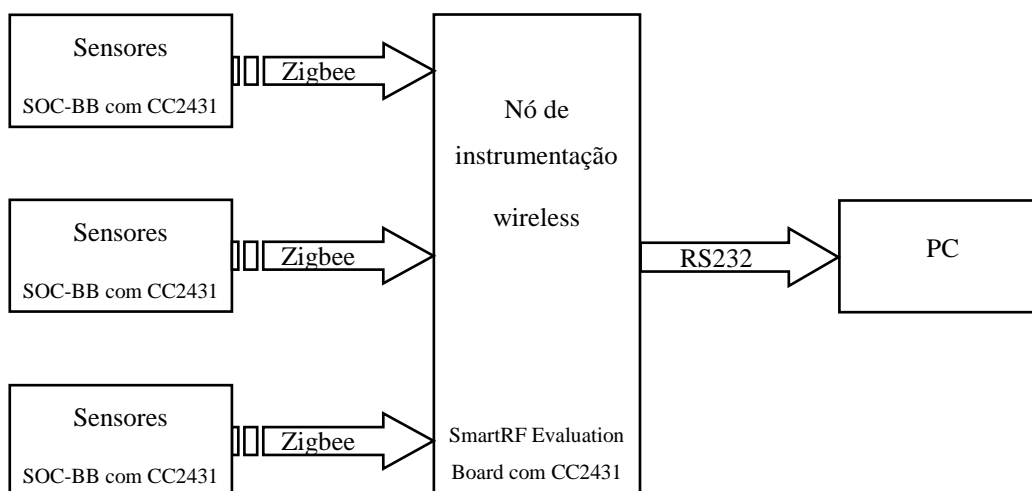
Figura 4.2 - Modelo do sistema de instrumentação distribuída proposto

O *hardware* é baseado numa solução para IEEE 802.15.4/Zigbee do tipo SOC da Texas Instruments, o CC2431 EM (Evaluation Module) (Figura 4.3) [34], cujas principais características são a seguir mencionadas.

Figura 4.3 - O CC2431 EM

Rádio frequência:

- *Transceiver* RF segundo o standard IEEE 802.15.4 (2,4 GHz)

Microcontrolador:

- Núcleo do tipo 8051
- Memória Flash de 128 kB
- Memória RAM de 8 kB, dos quais 4 kB com retenção de dados
- Funcionalidade DMA
- *Timer watchdog*
- *Timer* MAC IEEE 802.15.4
- *Timer* genérico de 16 bits
- 2 timers genéricos de 8 bits
- *Hardware* de suporte de *debug*

Periféricos:

- *Hardware* de suporte CSMA/CA
- Suporte digital de RSSI/LQI
- Monitor de bateria e sensor de temperatura
- Conversor AD delta sigma de 12 bits e 8 entradas, com resolução configurável
- Coprocessador de segurança AES de 128 bits
- 2 USARTs com suporte para vários protocolos de comunicação série

- 21 pinos de I/O gerais, 2 dos quais com capacidade de entrada em corrente 20mA
- Núcleo 8051 com 32 kbytes de memória Flash

Módulo sensor

O módulo sensor, daqui para a frente denominado de *end device*, é desenvolvido numa SOC-BB (Figura 4.4) [34]. Esta placa é de dimensões reduzidas e é alimentada através de duas pilhas do tipo AA.
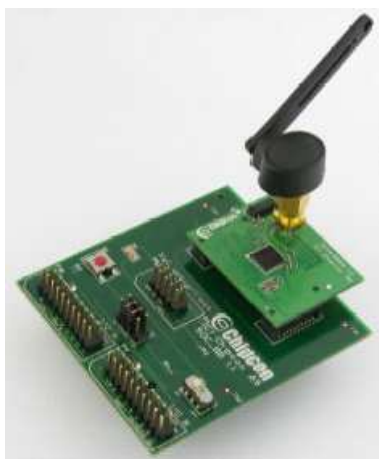
Figura 4.4 - SOC-BB com CC2431 EM

Os dados a serem monitorizados são a temperatura ambiente e o nível da tensão de alimentação da placa de monitorização. Esta última medição é muito importante neste trabalho, uma vez que as placas onde estão incorporados/ligados os sensores são alimentadas por pilhas do tipo AA, o que permite a total mobilidade das mesmas. Para assegurar o correcto funcionamento das placas é essencial monitorizar o nível da sua tensão de alimentação, para garantir que o seu valor se encontra dentro do intervalo indicado pelo fabricante (2 a 3,6 V).

Os sensores utilizados são os sensores incorporados na própria placa, sendo um de temperatura e outro do nível da bateria, e ainda um sensor de temperatura de precisão, externo à placa.

Para calibração dos sensores de temperatura incorporados nos módulos CC2431, deste ponto para a frente denominados por sensores de temperatura internos, deve-se recorrer a sensores de temperatura externos às placas, daqui para a frente denominados por

sensores de temperatura externos, que devem ser de precisão, para dessa forma estar disponível uma calibração mais eficiente dos sensores internos.

O sensor externo utilizado é o LM35 da National Semiconductor (Figura 4.5) [46], que tem as seguintes características:

- Calibrado directamente em Celsius;
- factor de escala linear (+ 10,0 mV por 1 ºC);
- exactidão de ± 0,5 ºC (a 25 ºC);
- gama de valores entre -55 º e 150 ºC;
- adequado para a utilização em aplicações remotas;
- tensão de alimentação entre 4 e 30 V;
- corrente de dreno inferior a 60 μA;
- baixo auto-aquecimento (0.08 ºC ao ar);
- Não linearidade típica de ± ¼ ºC;
- Baixa impedância de saída (0,1 Ω por 1 mA).
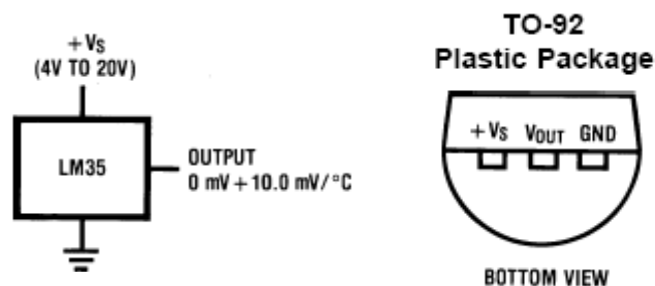
Figura 4.5 - O sensor LM35

Este sensor é implementado num circuito cuja saída é ligada a uma entrada do conversor AD do CC2431, o pino 0 do porto 0 (figura 4.6).
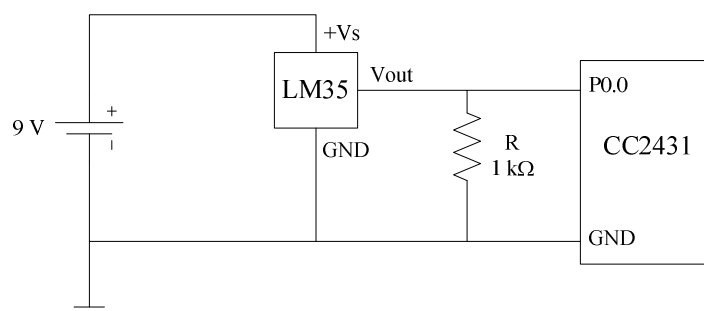
Figura 4.6 - O circuito de condicionamento de sinal

O conversor AD

O conversor AD do CC2431 é do tipo sigma-delta e suporta conversões até 12 bits (figura 4.7) [32]. O ADC inclui um *multiplexer* analógico até 8 canais configuráveis individualmente e um gerador de tensão de referência. Os resultados da conversão são escritos na memória através do DMA.

As entradas analógicas permitem a ligação de quase todo o tipo de sensores, ficando apenas excluídos da utilização os sensores não lineares.
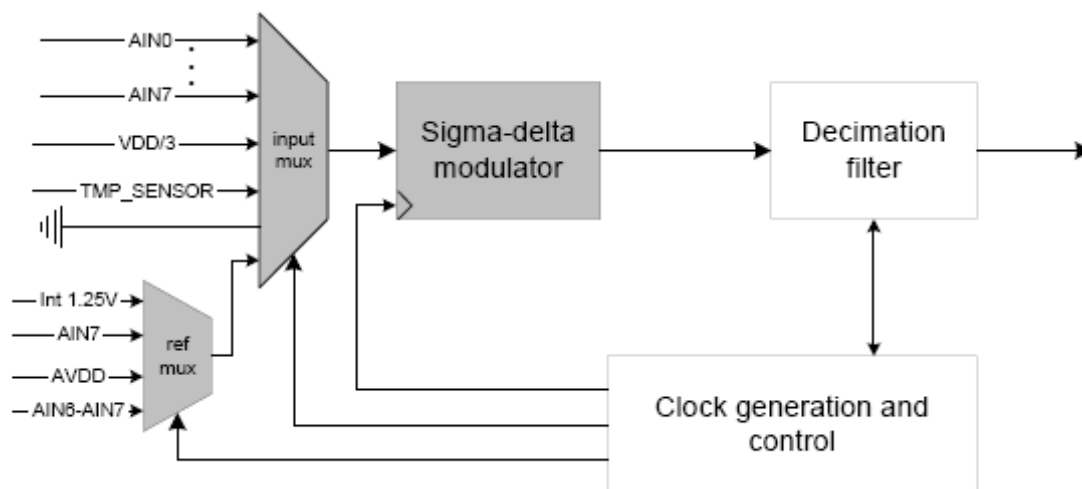
Figura 4.7 - Diagrama de blocos do conversor AD do CC2431

Conversor AD sigma delta

Este conversor AD sigma-delta tem basicamente dois módulos: o modulador e o filtro digital (Figura 4.8) [44].
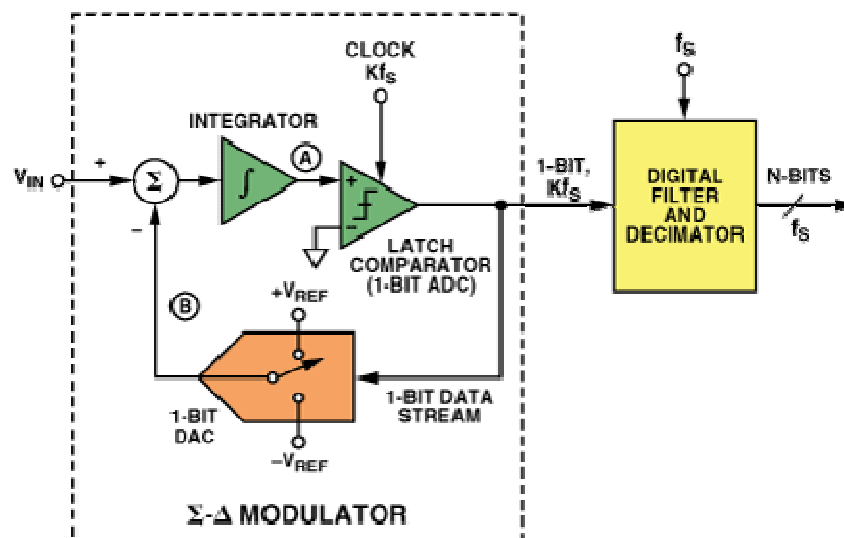
Figura 4.8 - Diagrama de blocos do conversor AD sigma-delta

O modulador baseia-se num conjunto composto por um integrador e um comparador de 1 bit e num conversor DA de 1 bit (Figura 4.9) [45].
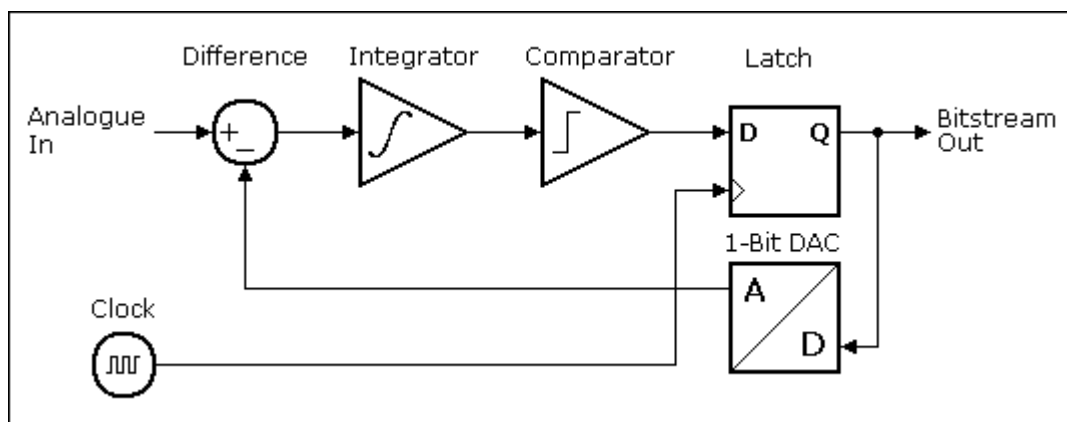
Figura 4.9 - Diagrama de blocos do modulador integrado no ADC sigma-delta

A saída do modulador é uma cadeia de bits. Devido ao feedback negativo, o valor médio do sinal à saída do conversor DA (figura 4.6) tende a ser igual ao valor do sinal à entrada do conversor (V_{IN}).

Se V_{IN} é zero, isto é, se tem o valor correspondente ao meio da escala, a cadeia de bits tem um número igual de 1s e de 0s.

À medida que o valor do sinal de entrada aumenta, o número de 1s aumenta, enquanto o número de 0s diminui.

Quando o sinal de entrada diminui então o número de 1s diminui, enquanto o número de 0s aumenta.

A densidade de 1s, isto é, a taxa de 1s existentes na cadeia relativamente ao número total de amostras no mesmo intervalo deve ser proporcional ao valor DC da entrada.

Entradas do ADC

Os sinais nos pinos do porto 0 podem ser utilizados como entradas ADC. A partir deste ponto, estes pinos serão referidos como pinos AIN0 – AIN7.

Estes pinos estão ligados ao ADC que, por sua vez, pode ser configurado para executar automaticamente uma sequência de conversões e, opcionalmente, depois de finalizada essa sequência, executar ainda uma conversão extra.

É possível configurar as entradas como *single-ended* ou como diferenciais. No caso de serem seleccionadas entradas do tipo diferencial estas consistem nos pares : AIN0-1,

AIN2-3, AIN4-5 e AIN6-7. A diferença entre as tensões aplicadas a estes pinos é a tensão diferencial, que é convertida pelo ADC.

De notar que em ambos os casos não pode ser aplicada nem uma tensão negativa a estes pinos, nem uma tensão maior que $V_{DD,}$ que corresponde à tensão de alimentação do CC2431, cujo valor deve estar regulado dentro do intervalo entre 2 e 3,6 V.

Adicionalmente, pode ser seleccionada como entrada do ADC a saída de um sensor de temperatura on-chip para medição de temperatura.

Também é possível seleccionar a tensão correspondente ao AVDD_SOC/3 como entrada do ADC. Esta entrada permite a implementação de um monitor de bateria em aplicações onde esta função for requerida.

Todas estas configurações são controladas pelo registo ADCCON2.SCH.

No trabalho desenvolvido foram seleccionadas as seguintes entradas:

- a entrada AIN0 para conversão da tensão à saída do circuito de condicionamento de sinal do sensor de temperatura LM35;
- a entrada do sensor de temperatura on-chip, daqui para a frente denominado como sensor de temperatura interno, e
- a entrada do AVDD_SOC/3, para monitorização da bateria do SOC_BB.

Tensão de referência

A tensão de referência para as conversões AD é seleccionável, podendo ser utilizada uma das seguintes tensões: a tensão de 1,25 V gerada internamente, a tensão do pino AVDD_SOC, uma tensão externa aplicada ao pino de entrada AIN7, ou uma tensão diferencial resultante das tensões aplicadas aos pinos AIN6 e 7.

Neste trabalho foi utilizada a tensão de referência interna de 1,25 V.

Temporização da conversão AD

O ADC deve funcionar com o clock do CC2431 a 32 MHz. Este valor dividido por 8 dá 4 MHz, que corresponde a um período de 0,25 μs. Tanto o modulador delta sigma como o filtro de decimação necessitam do clock a 4 MHz para os seus cálculos. A utilização de outras frequências afecta não só os resultados, mas também o tempo de conversão.

Quando é inicializada uma conversão a entrada do multiplexer dispõe de um tempo correspondente a 16 períodos do clock de 4 MHz para seleccionar o canal para conversão.

A taxa de decimação corresponde ao tempo, isto é, ao número de períodos do clock de que o filtro de decimação dispõe para calcular o resultado da conversão.

O tempo total requerido para executar uma conversão depende da taxa de decimação seleccionada e do tempo disponibilizado para a selecção do canal. O tempo total de conversão é calculado através da seguinte equação:

$$T_{conversão} = \left(taxa_{decimação} + 16\right) \times 0{,}25\ \mu s$$

Neste trabalho foi seleccionada a taxa de 512, o que significa que o filtro de decimação utiliza 512 períodos do clock de 4 MHz para calcular o resultado. Então para a taxa de decimação seleccionada, o tempo de conversão é:

$$T_{conversão} = \left(512 + 16\right) \times 0{,}25\ \mu s = 132\ \mu s$$

Esta taxa de decimação garante uma resolução de 12 bits, que é a melhor resolução disponibilizada pelo ADC do CC2431 (tabela 4.1), no entanto o tempo de conversão é o maior. As restantes taxas disponibilizadas pelo ADC do CC2431 permitem conversões mais rápidas, mas as correspondentes resoluções são mais baixas.

Tabela 4.1 - Taxas de decimação disponíveis no ADC do CC2431

Taxa de decimação	Resolução (bits)	Tempo de conversão (µs)
64	7	20
128	9	36
256	10	68
512	12	132

A escolha da taxa de decimação é uma questão muito importante na monitorização e/ou controlo de sistemas. Consoante as características das variáveis a monitorizar, é necessário ponderar entre a resolução dos valores obtidos e o tempo de resposta do sistema. O trabalho desenvolvido prevê a monitorização da temperatura ambiente e do nível da tensão da bateria, sendo ambas variáveis que alteram lentamente, logo o tempo de conversão do ADC não implica respostas desactualizadas do sistema. Sendo assim optou-se pela taxa de 512, que permite uma maior resolução dos valores obtidos. Como esta solução é a que tem uma performance menos interessante no que respeita ao tempo de resposta, a escolha desta taxa de decimação teve como objectivo testar a pior hipótese em

termos de tempo de resposta e a sua interferência no tempo de resposta do sistema desenvolvido.

Registos do ADC

O ADC tem os seguintes registos: dois registos de dados e três registos de controlo. A seguir é efectuada uma breve descrição dos mesmos.

Registos de dados

O ADC tem 2 registos de dados: ADCL (tabela 4.1) e ADCH (tabela 4.2). Nestes registos é colocado o resultado da conversão.

O registo ADC Data Low (0xBA) recebe a parte menos significativa do resultado da conversão.

Tabela 4.2 - Registo ADCL

Bit	Nome	Reset	R/W	Descrição
7:2	ADC[5:0]	0x00	R	Bits 5 a 0 do resultado da conversão
1:0	-	00	R0	Não utilizado. Lê sempre 0.

O registo ADC Data High (0xBB) recebe a parte mais significativa do resultado da conversão.

Tabela 4.3 - Registo ADCH

Bit	Nome	Reset	R/W	Descrição
7:0	ADC[13:6]	0x00	R	Bits 13 a 6 do resultado da conversão

Registos de controlo

O ADC tem 3 registos de controlo: ADDCON1 (tabela 4.3), ADDCON2 (tabela 4.4) e ADCCON3 (tabela 4.5). Estes registos são utilizados para configurar o ADC e para reportar estados.

O registo ADC CONTROL 1 (0xB4) é utilizado para configurar o ADC e para reportar estados.

O bit ADDCON1.EOC é um bit de estados que fica a 1 quando uma conversão acaba e fica a 0 quando o ADC está a ser lido.

O bit ADDCON1.ST é utilizado para iniciar uma sequência de conversões. A sequência tem início quando este bit é colocado a 1, os bits ADCCON1.STSEL estão a 11 e não está a decorrer nenhuma conversão. Quando a sequência é completada este bit passa automaticamente a 0.

Os bits ADCCON1.STSEL seleccionam o evento que vai despoletar o início de uma nova sequência de conversões.

Nas tabelas seguintes, que resumem as opções dos registos de controlo, a coluna "Opção" indica, sempre que aplicável, a opção seleccionada no trabalho desenvolvido.

Tabela 4.4 - Registo ADDCON1

Bit	Nome	Reset	R/W	Descrição	Opção
7	EOC	0	R	Fim de conversão. Mantém-se a 0 se é completada uma nova conversão mas os dados da anterior ainda não foram lidos 0 – conversão não completada 1 – conversão completada	-
6	ST	0	R/W	0 – não há conversão a decorrer 1 – inicia uma sequência de conversão se ADDCON1.STSEL=1 e não há nenhuma conversão a decorrer	-
5:4	SISEL[1:0]	11	R/W	Selecciona o evento que inicia uma sequência de conversões 00 – trigger exterior no pino P2_0 01 – não espera por nenhum trigger 10 – trigger no *timer*1 channel 0 compare event 11 – trigger no ADCCON.ST=1	01
3:2	RCTR[1:0]	00	R/W	Controla o gerador aleatório de números de 16 bits 00 – operação normal (13x unrolling) 01 – no unrolling 10 – reservado 11 – o gerador está off	-
1:0	-	11	R/W	reservado	-

O registo ADC CONTROL 2 (0xB5) controla o modo como a sequência de conversões é executada.

Os bits ADDCON2.SREF são utilizados para seleccionar a tensão de referência utilizada na sequência de conversões.

Os bits ADDCON2.SDIV seleccionam a taxa de decimação e, consequentemente, a resolução, o tempo necessário para completar uma conversão e a taxa de amostragem.

Tabela 4.5 - Registo ADDCON2

Bit	Nome	Reset	R/W	Descrição	Opção
7:6	SREF[1:0]	00	R/W	Selecciona a tensão de referência utilizada na sequência de conversões 00 – tensão de referência interna de 1,25 V 01 – tensão de referência externa no pino AIN7 10 – tensão de referência externa no pino AVDD_SOC 11 – tensão de referência externa na entrada diferencial AIN6-7	00
5:4	SDIV[1:0]	01	R/W	Estabelece a taxa de decimação e a correspondente resolução para os canais incluídos na sequência de conversões 00 – taxa de 64 (resolução de 7 bits) 01 – taxa de 128 (resolução de 9 bits) 10 – taxa de 256 (resolução de 10 bits) 11 – taxa de 512 (resolução de 12 bits)	11
3:0	SCH[3:0]	0000	R/W	Selecciona a sequência de canais para conversão 0000 – AIN0 0001 – AIN1 0010 – AIN2 0011 – AIN3 0100 – AIN4 0101 – AIN5 0110 – AIN6 0111 – AIN7 1000 – AIN0-1 1001 – AIN2-3 1010 – AIN4-5 1011 – AIN6-7 1100 – GND 1101 – tensão de referência interna 1,25 V 1110 – sensor de temperatura interno 1111 – VDD/3	0000

O registo ADC CONTROL 3 (0xB6) controla as características da conversão extra, que tem lugar a seguir à sequência de conversões, logo após este registo ser actualizado. O código dos bits deste registo é igual ao dos bits do ADCCON2.

Tabela 4.6 - Registo ADDCON3

Bit	Nome	Reset	R/W	Descrição	Opção
7:6	EREF[1:0]	00	R/W	Selecciona a tensão de referência utilizada na conversão extra 00 – tensão de referência interna de 1,25 V 01 – tensão de referência externa no pino AIN7 10 – tensão de referência externa no pino AVDD_SOC 11 – tensão de referência externa na entrada diferencial AIN6-7	00
5:4	EDIV[1:0]	00	R/W	Estabelece a taxa de decimação e a correspondente resolução para os canais incluídos na sequência de conversões 00 – taxa de 64 (resolução de 7 bits) 01 – taxa de 128 (resolução de 9 bits) 10 – taxa de 256 (resolução de 10 bits) 11 – taxa de 512 (resolução de 12 bits)	11
3:0	ECH[3:0]	0000	R/W	Selecciona a sequência de canais para a conversão extra 0000 – AIN0 0001 – AIN1 0010 – AIN2 0011 – AIN3 0100 – AIN4 0101 – AIN5 0110 – AIN6 0111 – AIN7 1000 – AIN0-1 1001 – AIN2-3 1010 – AIN4-5 1011 – AIN6-7 1100 – GND 1101 – tensão de referência interna 1,25 V 1110 – sensor de temperatura interno 1111 – VDD/3	1110/1111

Resultado da conversão AD

O resultado da conversão AD é representado na forma de complemento para 2. No caso das conversões *single-ended*, isto é, quando as conversões não utilizam as entradas

diferenciais, o resultado é sempre positivo. Isto acontece porque o resultado é a diferença entre a massa e o sinal de entrada, que é sempre positivo.

$$V_{conversão} = V_{input} - V_{inn} \text{ ; onde } V_{inn} = 0 \text{ V}$$

O valor máximo é atingido quando a amplitude da entrada é igual à tensão de referência V_{REF}. No trabalho efectuado foi utilizada a configuração single-ended e a entrada seleccionada foi o pino 0 do porto 0.

Nas configurações diferenciais a diferença entre os pares de pinos são convertidas, podendo esta diferença ser negativa.

O resultado da conversão digital está disponível nos registos de dados ADCH e ADCL, mas apenas quando o bit ADCCON1.EOC fica a 1.

A tabela 4.7 representa o conjunto dos registos ADCH e ADCL, daqui para a frente denominado de ADCR, que forma uma palavra de 16 bits. O bit mais significativo representa o sinal do resultado da conversão AD. Como neste trabalho é utilizada uma entrada single ended (AIN0) então o resultado da conversão AD é sempre positivo, logo este bit está sempre a 0.

Tabela 4.7 - Representação do resultado da conversão AD

ADCR															
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
ADCH								ADCL							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Resultado da conversão															
0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1

Pode-se então concluir que ADCR tem $2^{15} = 32768$ níveis para representar o resultado da conversão AD.

A seguir são apresentados os cálculos efectuados para determinar a resolução dos três elementos monitorizados no sistema implementado.

Resolução dos elementos monitorizados

O valor seleccionado para a tensão de referência do ADC é 1,25 V, o que significa que o conversor pode converter valores entre 0 e 1,25 V, sendo esta gama de tensões representada em 32768 níveis, considerando os 15 bits do ADCR. Partindo deste pressuposto pode-se determinar a resolução obtida pelo ADC nas condições estabelecidas.

$$\begin{array}{ccc} 1{,}25\ \text{V} & - & 32768\ \text{níveis} \\ \text{x} & - & 1\ \text{nível} \end{array}$$

$$x = \frac{1{,}25}{32768} = 38{,}1\ \mu\text{V/nível}$$

Pelo cálculo anterior verifica-se que, nas condições previamente estabelecidas, a resolução do ADC é de 38,1 µV/nível, isto é, a menor variação de tensão na entrada do ADC que produz uma variação de um nível na sua saída é 38,1 µV.

Nível da bateria

Segundo o fabricante, o valor da tensão de alimentação da placa (V_{DD}) pode variar entre 2 e 3,6 V, de forma a garantir o seu correcto funcionamento. A tensão monitorizada é $V_{DD/3}$, o que significa que os valores à entrada do ADC podem variar entre 0,67 e 1,2 V (2/3 e 3,6/3 V, respectivamente). Conclui-se então que o valor máximo da tensão monitorizada é ligeiramente menor que o triplo do valor máximo da tensão de referência.

$$3{,}6 < 3{,}75\ \ (3 \times 1{,}25)\ \ \text{(V)}$$

Pode-se então considerar uma gama de valores medidos no ADC entre 0 e 3,75 V, sabendo a priori que a mesma não será utilizada na totalidade, uma vez que o valor máximo será 3,6 V e o valor mínimo de 2 V não pode ser atingido, devendo as pilhas ser substituídas antes de esse valor ser atingido.

Tendo em conta as considerações anteriores, pode-se determinar a resolução correspondente à monitorização da bateria.

$$\begin{array}{ccc} 3{,}75\ \text{V} & - & 32768\ \text{níveis} \\ x & - & 1\ \text{nível} \end{array}$$

$$x = \frac{3{,}75}{32768} = 114{,}4\ \mu\text{V/nível}$$

Pode-se então concluir que a resolução do sistema de monitorização da bateria é de 114,4 μV/nível.

Sensores de temperatura internos

Para a conversão dos valores obtidos através dos sensores de temperatura internos foi seleccionada a tensão interna de 1,25 V, o que implica que a gama de tensões convertida pelo ADC varia entre 0 e 1,25 V.

O coeficiente de temperatura destes sensores é 2,4 mV/ºC, o que significa que por cada grau Celsius na entrada do sensor obtém-se na sua saída 2,4 mV. Sabendo o coeficiente de temperatura do sensor pode-se determinar a equivalência entre a temperatura medida à entrada do sensor em graus Celsius e o número de níveis à saída do ADC, considerando os 15 bits.

$$1{,}25\ \text{V} - 32768\ \text{níveis}$$

$$1\ ^{\circ}\text{C} - 0{,}0024\,\text{V} - \quad x$$

$$x = \frac{0{,}0024 \times 32768}{1{,}25} = 62{,}9\ \text{níveis}/^{\circ}\text{C}$$

Concluindo, no caso do sistema de monitorização da temperatura ambiente através dos sensores de temperatura internos do CC2431, uma variação de 1 ºC na entrada do sensor produz uma variação de 62,9 níveis na saída do ADCR, logo a resolução deste sistema é de $15{,}9 \times 10^{-3}\ ^{\circ}\text{C/nível}$.

É de realçar o facto de ter havido necessidade de calibrar quase todos os sensores internos, pois estes, mesmo após corrigido o offset indicado pelo fabricante (0,743 V), apresentavam valores diferentes dos obtidos através dos sensores externos, sendo essas diferenças da ordem das unidades. No entanto, essa diferença está contemplada pelo fabricante, pois prevê um erro máximo de ±2 ºC para temperaturas entre -20 e 80 ºC. A calibração foi efectuada através do *software*, uma vez que este era o procedimento aconselhado pelo fabricante.

Sensores de temperatura externos

Para a conversão dos valores obtidos através dos sensores de temperatura externos foi seleccionada a tensão interna de 1,25 V, pelo que a gama de tensões varia entre 0 e 1,25V, tal como nas monitorizações referidas anteriormente.

O coeficiente de temperatura dos sensores é 10 mV/ºC, o que significa que 1 ºC na entrada do sensor equivale a 10 mV da tensão à entrada do ADC. Pode-se determinar a equivalência entre a temperatura em graus Celsius à entrada do sensor e o número de níveis à saída do ADC, considerando os 15 bits.

$$1{,}25 \text{ V} - 32768 \text{ níveis}$$
$$1\,^{\circ}\text{C} - 0{,}010\text{V} - x$$
$$x = \frac{0{,}010 \times 32768}{1{,}25} = 262{,}1 \text{ níveis}/^{\circ}\text{C}$$

Concluindo, no caso do sistema de monitorização da temperatura ambiente com recurso aos sensores de temperatura LM35, cada grau Celsius equivale a 262,1 níveis do ADCR, o que corresponde a uma resolução de $3{,}81 \times 10^{-3}\ ^{\circ}\text{C/nível}$.

Nó de instrumentação

O nó de instrumentação, deste ponto para a frente denominado como colector, é desenvolvido numa SmartRF EB (Evaluation Board) (Figura 4.8) [34]. Esta placa pode ser alimentada através da ligação USB, facto que permite que a mesma esteja apenas dependente do PC.

Figura 4.10 - SmartRF EB com CC2431 EM

A possibilidade de comunicação através da porta série é bastante importante neste trabalho, uma vez que é através desta que é efectuada a transmissão de dados entre esta placa e o PC. Isto permitirá, não só a monitorização dos vários elementos, como o tratamento dos dados (por exemplo para posterior controlo) ou até o acesso aos mesmos num ponto remoto através da Internet, bastando para isso implementar no PC uma aplicação do tipo *Webserver*.

Uma vez seleccionado o *hardware*, vai-se realizar uma análise à plataforma de *software*. Essa análise será efectuada na secção seguinte.

4.4.2 Plataforma de *software*

A aplicação foi desenvolvida a partir da *stack* IEEE 802.15.4/Zigbee implementada pela Chipcon/Texas Instruments.

Foi desenvolvida em C/C++, tendo sido utilizado o IAR da IAR Systems.

Nas secções seguintes são apresentadas as funções atribuídas a cada componente da rede, sendo ainda apresentado um fluxograma que descreve a sequência de operações realizadas por cada componente.

Comunicação entre os componentes da rede sem fios

A comunicação sem fios é efectuada segundo o protocolo IEEE 802.15.4/Zigbee, entre o *end device* e o colector, tendo como objectivo a transferência de dados provenientes dos sensores implementados no *end device*.

Colector

O colector pode ser um coordenador ou um *router*. As características destes elementos são iguais, exceptuando a capacidade de criação de uma rede Zigbee, que é exclusiva do coordenador.

Coordenador

O coordenador tem as seguintes funções:

- Criar a rede Zigbee, permitindo a integração de *router*s e *end device*s;
- Permitir o *binding* de *end device*s, para recepção de dados;

- Receber dados provenientes dos *end devices*, com recurso ao protocolo Zigbee e
- Transmitir os dados para o PC recorrendo ao protocolo RS232.

A sequência de operações realizadas pelo coordenador está ilustrada no fluxograma da figura 4.11.
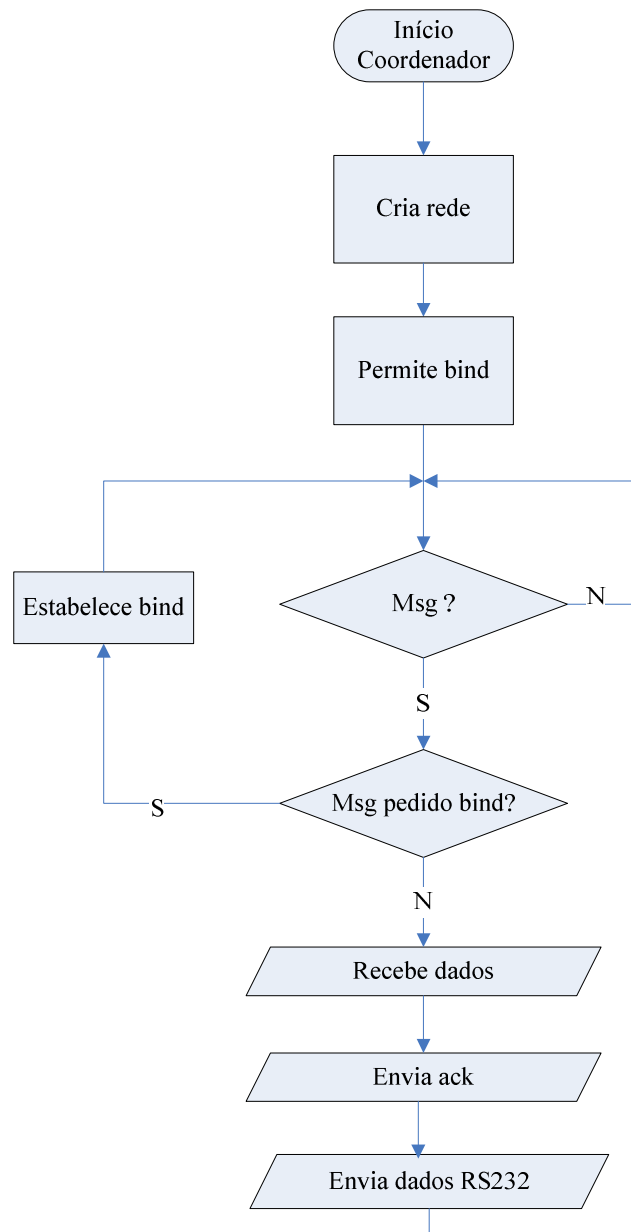
Figura 4.11 - Fluxograma do coordenador

Router

O *router* tem as seguintes funções:

- Integrar a rede Zigbee;

- Permitir o *binding* de *end device*s, para recepção de dados;
- Receber dados provenientes dos *end device*s, com recurso ao protocolo Zigbee e
- Transmitir os dados para o PC recorrendo ao protocolo RS232.

A sequência de operações realizadas pelo coordenador está ilustrada no fluxograma da figura 4.12.
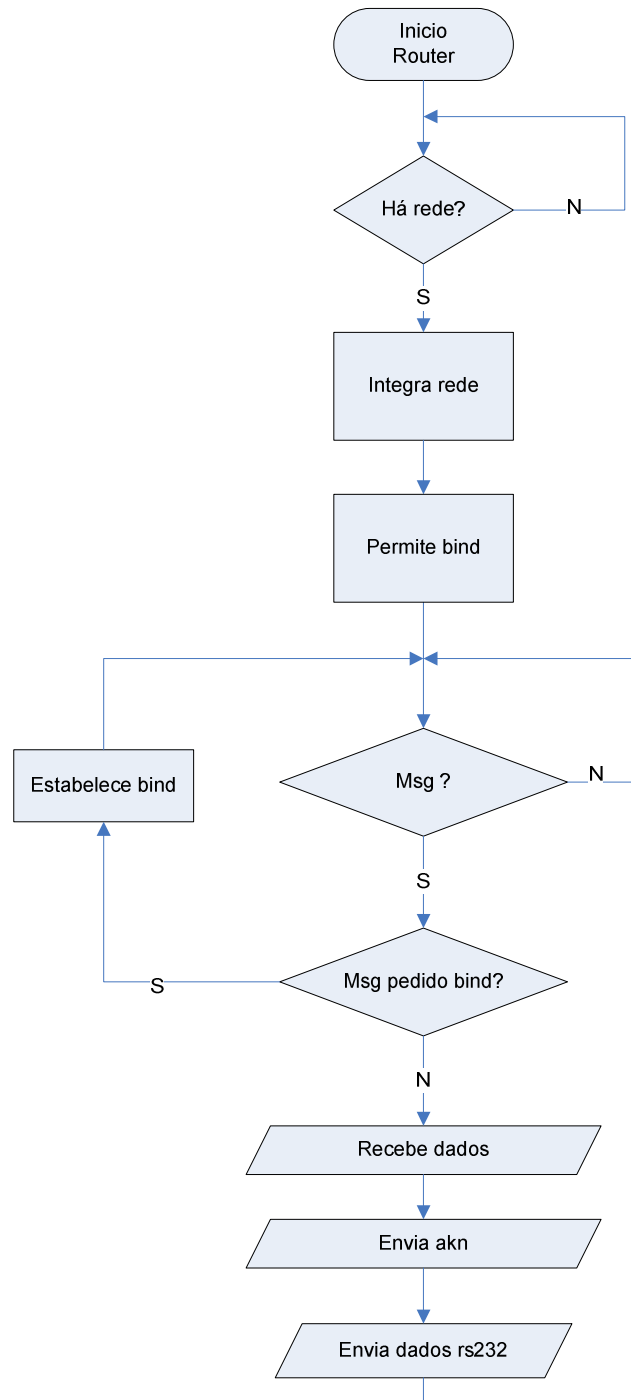
Figura 4.12 - Fluxograma do *router*

End device

O *end device* tem as seguintes funções:

- Integrar a rede Zigbee;
- Proceder ao *binding* com o colector (coordenador ou *router*) depois de o mesmo o ter permitido e
- Transmitir os dados provenientes dos sensores, com recurso ao protocolo Zigbee.

A sequência de operações realizadas pelo coordenador está ilustrada no fluxograma da figura 4.13.
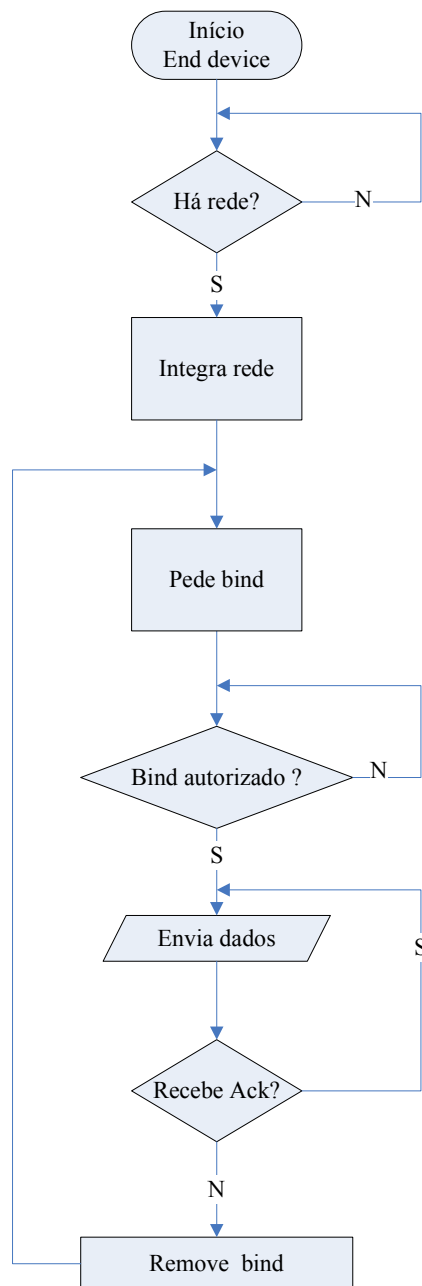
Figura 4.13 - Fluxograma do *end device*

As operações de aquisição de sinal e envio de dados efectuadas pelo *end device*, denominadas genericamente no fluxograma anterior por “envia dados”, são descritas mais pormenorizadamente no fluxograma seguinte [figura 4.14].
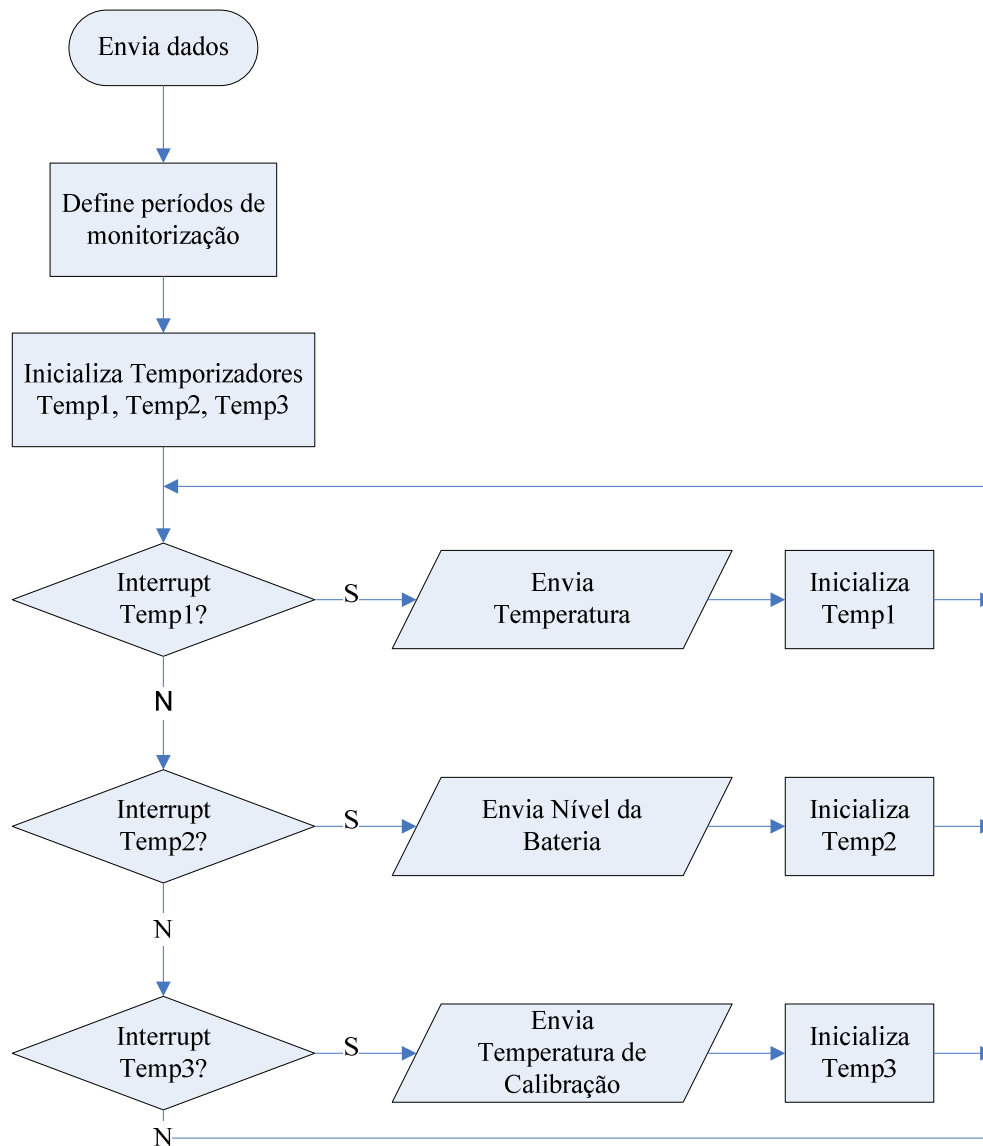
Figura 4.14 - Fluxograma do envio de dados no *end device*

4.4.3 A Z-stack

A Z-stack é uma implementação da Texas Instruments baseada na especificação Zigbee. Está certificada como Zigbee Compliant Platform pela Zigbee Alliance. Consiste nos seguintes componentes:

- OSAL
- *Stack* Zigbee
- *Stack* IEEE 802.15.4 MAC
- Aplicação
- MT (Monitor Test)

São fornecidos os seguintes serviços com a aplicação:

- Inicialização
- Configuração
- Descoberta – descoberta de componente, de rede e de serviço
- Transferência de dados

Gestão dos componentes numa rede

Cada componente tem um conjunto de parâmetros de configuração que podem ser configurados através de um computador ou de um microcontrolador externo. Estes parâmetros de configuração têm valores por defeito que são definidos no código. Cada parâmetro de configuração específico da rede deve ter o mesmo valor em todos os componentes da rede. Quanto aos parâmetros de configuração específicos do componente podem ter valores diferentes em cada componente da rede.

O parâmetro ZCD_NV_LOGICAL TYPE deve ser configurado de forma que:

1 Exista exactamente um coordenador;

2 Todos os componentes alimentados através de pilhas têm de ser configurados como *end-devices*.

Depois de o coordenador iniciar a rede todos os componentes podem encontrá-la e integrar-se.

O coordenador verifica todos os canais especificados no ZCD_NV_CHANLIST e escolhe o nível de energia baixo. Em caso de empate, escolhe o canal com o menor número de redes Zigbee existentes. Depois de escolher o canal, o coordenador escolhe o identificador de rede, que será identificado pelo parâmetro ZCD_NV_PANID.

Os *router*s e os *end-devices* verificam os canais especificados nos respectivos ZCD_NV_CHANLIST e procuram a rede com o identificador especificado pelo parâmetro ZCD_NV_PANID.

O *binding* entre componentes

Um *binding* é uma ligação lógica estabelecida entre dois componentes no nível de aplicação.

Podem ser criados múltiplos *binding*s num componente, um para cada tipo de pacote de dados. Um *binding* pode ter mais do que um componente destino, sendo denominado de *binding* do tipo um-para-muitos. Isto permite que a aplicação envie os dados sem necessitar de saber o endereço de destino. Neste caso, depois de o *binding* estar criado no componente fonte, a aplicação pode enviar dados sem especificar o endereço de destino. Isto obriga a *stack* a procurar o destino na tabela interna de *binding*, baseada no identificador de comando do pacote. No caso de haver mais do que um destino na entrada de *binding*, a *stack* envia uma cópia para cada destino especificado na entrada.

Se a opção de NV_RESTORE estiver activada a *stack* grava as entradas de *binding* na RAM não volátil. Assim, se o componente necessitar de trocar de pilhas, ou se acontecer um *reset* acidental, o componente pode recuperar essa informação, não havendo necessidade de o utilizador efectuar o setup dos *binding*s.

Existem duas formas de configuração dos *binding*s:

- Se o endereço IEEE de 64 bits do destino é conhecido o zb_BindDeviceRequest pode criar uma entrada de *binding*;
- Se esse endereço não é conhecido o *binding* pode ser criado a partir de um pedido efectuado através do *hardware*.

Os *binding*s podem ser criados apenas entre componentes complementares, isto é, o *binding* só têm sucesso se ambos os componentes tiverem registado o mesmo command.id nas correspondentes estruturas de descrição e ainda se um componente tem o comando como output e o outro o tenha como input.

Desenvolvimento da aplicação a partir da Z-stack

Para se poder utilizar um perfil desenvolvido pela TI é necessário proceder à execução dos seguintes pontos:

1 Identificar todos os componentes existentes na aplicação

No trabalho desenvolvido: sensores de temperatura, monitor de bateria.

2 Identificar os comandos que necessitem de ser trocados entre os componentes e atribuir um comand.id a cada um.

No trabalho desenvolvido: leitura de temperatura interna, leitura de temperatura externa, leitura de tensão.

3 Para cada comando identificar se é entrada ou se é saída do componente.

Por exemplo:

A leitura de temperatura é saída do módulo onde está inserido o sensor de temperatura e entrada do colector.

4 Criar estruturas para cada componente que incluem os dados sobre o próprio componente, sobre a rede e ainda sobre os componentes que compõem a rede.

5 Para cada comando definir o formato da mensagem a ser trocada e a sua interpretação.

Por exemplo: o valor da temperatura pode ser trocado como um valor de 8 bits, 0 (00000000) indica 0 ºC e 255 (11111111) indica 64 ºC em intervalos de 0,25 ºC.

6 Efectuar o download da aplicação em cada componente.

O componente com comandos de saída deve gerar o pacote de dados ou periodicamente ou quando ocorre um evento externo.

O componente com comandos de entrada deve gerir a recepção de pacotes e analisar o payload de cada pacote recebido.

7 Identificar uma estratégia de *binding* de modo que os componentes possam trocar pacotes correctamente.

Requisitos da aplicação

Os requisitos da aplicação a desenvolver são os seguintes:

Os nós sensores registam medições da temperatura ambiente e do nível da bateria e enviam-nas para um nó colector.

O nó colector recebe a informação proveniente de todos os outros componentes da rede e envia-os para o PC via RS232, para armazenamento e posterior processamento *offline*.

Para aumentar a fiabilidade do sistema a rede pode ter mais do que um nó colector.

A aplicação deve ser capaz de:

- Formar uma rede automaticamente;
- Os componentes sensores devem descobrir e fazer o *bind* a um nó colector automaticamente, depois de integrados na rede;
- Os sensores devem enviar dados periodicamente ao nó colector com *acknowledge end to end*;
- Se o nó sensor não recebe um *acknowledge* do seu nó colector deve remover o *binding* e deve tentar nova descoberta e novo *bind* a possivelmente outro nó colector.

Esta aplicação tem duas configurações de componentes: o sensor e o colector.

O sensor é configurado como um *end device*, uma vez que os sensores são tipicamente alimentados por pilhas.

O colector é configurado como coordenador. No caso de haver mais do que um nó colector, então deve ser observada a seguinte regra: deve ser configurado apenas um colector como coordenador da rede, que tem de ser o que inicializa a rede. Os colectores que posteriormente integrem a rede terão de ser configurados como *routers*.

Funções da aplicação

A Z-stack desenvolvida pela Chipcon/Texas Instruments baseia-se nas funções a seguir descritas.

A aplicação desenvolvida neste projecto baseia-se na Z-stack, logo também tem como base as mesmas funções.

Existem três tipos de funções:

- as funções API;
- as funções do tipo *callback*, que são as respostas às funções API e
- os parâmetros de configuração, que por sua vez também se podem dividir em dois tipos de parâmetros: os parâmetros específicos da rede e os parâmetros específicos do componente.

Funções API

Zb_systemReset

Esta função executa o *reset* do componente.

Zb_StartRequest

Esta função inicia a *stack* do protocolo Zigbee. Se as opções de *startup* indicam que o estado anterior da rede deve ser mantido (ACD_START_OPT_CLEAR_CONFIG ON) então o componente deve carregar o estado da rede e de seguida deve iniciar o funcionamento da mesma. Senão o componente deve iniciar uma rede, se estiver configurado como coordenador, ou deve tentar integrar uma existente, se estiver configurado como *router* ou como *end device*.

Zb_PermitJoiningRequest

Esta função é utilizada para controlo das permissões de *joining*, isto é, permite ou não que novos componentes integrem a rede.

zb_BindDevice

Esta função estabelece ou remove um *binding* entre dois componentes da rede. Depois de estabelecido o *binding*, uma aplicação do componente fonte pode enviar mensagens ao componente destino, referenciando o identificador de comando (commandID) do *binding*.

Os *binding*s são guardados na memória não volátil dos componentes e são restaurados depois de um *reset*, excepto se a opção de *startup* especifique o contrário. Desta maneira, um *reset* acidental, ou uma falha de energia temporária não afectam a aplicação.

zb_AllowBind

Esta função põe o componente no modo Allow Binding durante um determinado período de tempo.

zb_SendDataRequest

Inicia a transmissão de um pacote de dados para o componente *peer*. O destino da transmissão pode ser o endereço IEEE do componente *peer*, ou um endereço inválido. Neste caso, o pacote deve ser enviado para todos os componentes da rede com *binding*s estabelecidos com o componente fonte, identificados com o commandID especificado.

Esta função tem retorno imediato. O estado da operação retorna através da função de *callback* zb_SendDataConfirm.

zb_ReadConfiguration

Esta função é utilizada para ler as propriedades da configuração na memória não volátil.

zb_WriteConfiguration

Escreve as propriedades da configuração na memória não volátil.

zb_GetDeviceInfo

Permite obter informação acerca das propriedades de um componente da rede.

zb_FindDeviceRequest

Esta função é utilizada para determinar o endereço reduzido de um componente da rede. O componente que inicia a chamada para esta função e o componente a ser descoberto têm de ser membros da mesma rede. Quando o componente é descoberto é chamada a função de *callback* zb_FindDeviceConfirm.

A tabela seguinte resume as características principais das funções API

Tabela 4.8 - Resumo das funções API

Função	Protótipo	Parâmetros	Valor de retorno
zb_SystemReset	void zb_systemReset (void)	nenhum	nenhum
zb_StartRequest	void zb_StartRequest (void)	nenhum	nenhum
zb_PermitJoiningRequest	void zb_PermitJoiningRequest (uint16 destination, uint8 timeout)	destination, timeout	ZB_SUCCESS/erro
zb_*Bind*Device	uint8 zb_*Bind*Device (uint8 create, uint16 commandID, uint8 *pDestination)	create, commandID, pDestination	nenhum
zb_Allow*Bind*	void zb_Allow*Bind* (uint16 commandID, uint8 timeout)	commanID, timeout	nenhum
zb_SendDataRequest	void zb_SendDataRequest (uint16 destination, uint16 commandID, uint8 len, uint8 *pData, uint8 handle, uint ack, uint8 radius)	destination, commandID, len, pdata, handle, txoptions, radius	nenhum
zb_ReadConfiguration	void zb_ReadConfiguration (uint8 configID, uint8 len, void * pvalue)	configID, len, pvalue	nenhum
zb_WriteConfiguration	void zb_ WriteConfiguration (uint8 configID, uint8 len, void * pvalue)	configID, len, pvalue	nenhum
zb_GetDeviceInfo	void zb_GetDeviceInfo (uint8 parameter, uint8 len, void *pvalue)	parameter, len, pvalue	nenhum
zb_FindDeviceRequest	void zb_FindDeviceRequest (uint8 searchtype, uint8 *searchkey)	searchtype, searchkey	nenhum

Funções de callback

Esta secção descreve sucintamente as funções do tipo *callback*.

zb_StartConfirm

Esta função é chamada pela *stack* depois de completada uma operação de Start Request e notifica a aplicação do estado dessa operação.

Se o estado é ZB_SUCCESS ON então o componente iniciou a rede, no caso de estar configurado como um coordenador, ou integrou a rede, se estiver configurado como um *router* ou como um *end device*.

zb_BindConfirm

Esta função é chamada pela *stack* depois de completada uma operação de *bind* e contém o estado dessa operação.

zb_AllowBindConfirm

Esta função é chamada pela *stack* quando um componente se encontra no modo Alow *Bind* e responde a um pedido de *bind* de outro componente da rede.

zb_SendDataConfirm

É chamada pela *stack* quando é completada uma operação de envio de dados.

No caso de o *acknowledge* estar activado, esta função não retorna sem que o *acknowledge* seja recebido, ou ocorra um timeout.

zb_ReceiveDataIndication

É chamada de forma assíncrona pela *stack* para notificar a aplicação quando são recebidos dados de um componente *peer*.

zb_FindDeviceConfirm

É chamada pela Z-stack quando é completada uma operação de Find Device.

zb_HandleKeys

É chamada pelo sistema operativo quando é activado um evento chave. Isto acontece quando é premido um botão da placa.

zb_HandleOsalEvent

É chamada pelo sistema operativo quando é activado um evento de tarefa.

A tabela seguinte resume as características das funções do tipo *callback*.

Tabela 4.9 - Resumo das funções callback

Função	Protótipo	Parâmetros
zb_StartConfirm	void zb_StartConfirm (uint8 status)	status
zb_*Bind*Confirm	void zb_*Bind*Confirm (uint16 commandID, uint8 status)	commandID, status
zb_Allow*Bind*Confirm	void zb_Allow*Bind*Confirm (uint16 source)	source
zb_SendDataConfirm	void zb_SendDataConfirm (uint8 handle, uint8 status)	handle, status
zb_ReceiveDataIndication	void zb_ReceiveDataIndication (uint16 source, uint16 commandID, uint8 len, uint8 * pData)	source, commandID, len, pData
zb_FindDeviceConfirm	void zb_FindDeviceConfirm (uint8 searchType, uint8*searchkey, uint8 *result)	searchType, searchkey, result
zb_HandleKeys	void zb_HandleKeys (uint8 shift, uint8 keys)	shift, keys
zb_HandleOsalEvent	void zb_HandleOsalEvent (uint16 event)	event

Parâmetros de configuração

O seguinte conjunto de propriedades de configuração pode ser escrito ou lido em memória não volátil, utilizando para isso as funções zb_WriteConfiguration e zb_ReadConfiguration.

Cada um dos parâmetros tem valores por defeito, que são definidos no código. Uma vez realizado o download da imagem do código no componente, os parâmetros são inicializados com esses valores.

Depois do componente ser programado, esses parâmetros podem ser alterados, ou pela própria aplicação, ou através de uma ferramenta compatível, instalada num computador ou num microcontrolador externo.

Quaisquer alterações nos parâmetros apenas têm efeito no componente depois de realizados um *reset* e um *restart* do mesmo.

É possível apagar todos os valores da configuração e restaurar os valores iniciais, bastando para isso fazer a activação apropriada do parâmetro de start_up_option.

Existem dois tipos de parâmetros de configuração: os parâmetros específicos da rede e os específicos do componente.

A seguir são descritos os vários parâmetros de configuração disponíveis na aplicação.

Parâmetros específicos da rede

Este parâmetro identifica a rede. Deve ter um valor entre 0 e 0x3FFF, se estiver a 0xFFFF indica que pode ser qualquer valor. Redes coexistentes devem ter diferentes valores.

Este parâmetro é uma máscara de bits dos canais nos quais a rede pode operar. Podem coexistir múltiplas redes.

ZCD_NV_PRECFGKEY

Este parâmetro contém a chave de 128 bits que é utilizada para segurança dos pacotes, caso essa funcionalidade esteja activada.

ZCD_NV_PRECFGKEYS_ENABLE

Se a funcionalidade segurança estiver activada existem duas opções para distribuir a chave de segurança por todos os componentes da rede.

ZCD_NV_SECURITY_LEVEL

Este parâmetro indica o nível de segurança aplicado a cada pacote, caso esta funcionalidade esteja activada. Varia entre 1 e 7.

Nos níveis 1 a 3 os pacotes não são encriptados, mas são autenticados com o código de autenticação de 4, 8, ou 16 bytes.

No nível 4 os pacotes são encriptados, mas não são autenticados.

Nos níveis 5 a 7 os pacotes são encriptados e são autenticados com códigos de autenticação de 4, 8, ou 16 bytes.

ZCD_NV_BCAST_RETRIES

Indica o número máximo de retransmissões que um componente pode tentar ao transmitir um pacote do tipo *broadcast*. Varia entre 1 e 3.

ZCD_NV_PASSIVE_ACK_TIMEOUT

Indica a quantidade de tempo (expressa em unidades de 100 ms) que um componente deve esperar para escutar dos nós vizinhos antes de proceder à retransmissão de um pacote *broadcast*.

ZCD_NV_BCAST_DELIVERY_TIME

Indica a quantidade de tempo (em unidades de μs) que um pacote *broadcast* demora a propagar na rede.

ZCD_NV_ROUTE_EXPIRY_TIME

Indica a quantidade de tempo (expressa em s) durante o qual um *router* deve estar *idle* (não pode transmitir pacotes).

A tabela 4.3 resume as características dos parâmetros de configuração específicos da rede.

Tabela 4.10 - Resumo dos parâmetros de configuração específicos da rede

Parâmetro	configID	Tamanho (bytes)	Valor por defeito	Ficheiro
ZCD_NV_PANID	0x0083	2	ZDAPP_CONFIG_PAN_ID	f8wconfig.cfg
ZCD_NV_CHANLIST	0x0084	4	DEFAULT_CHANLIST	f8wconfig.cfg
ZCD_NV_PRECFGKEY	0x0062	16	defaultkey[ ]	zglobals.c
ZCD_NV_PRECFGKEYS_ENABLE	0x0063	1	ZgPreConfigKeys	zglobals.c
ZCD_NV_SECURITY_LEVEL	0x0061	1	SECURITY_LEVEL	nwk_globals.h
ZCD_NV_BCAST_RETRIES	0x002E	1	MAX_BCAST_RETRIES	zglobals.h
ZCD_NV_PASSIVE_ACK_TIMEOUT	0x002F	1	PASSIVE_ACK_TIMEOUT	zglobals.h
ZCD_NV_BCAST_DELIVERY_TIME	0x0030	1	BCAST_DELIVERY_TIME	zglobals.h
ZCD_NV_ROUTE_EXPIRY_TIME	0x002C	1	ROUTE_EXPIRY_TIME	f8wconfig.cfg

Parâmetros específicos do componente

Parâmetros de *startup*

ZCD_NV_STARTUP_OPTION

Este parâmetro controla a lógica de *startup* do componente. Pode ter um dos seguintes valores:

0x01 - ZCD_STARTOPT_CLEAR_CONFIG – Nesta opção o componente procede ao overwrite de todos os seus parâmetros de configuração

0x02 - ZCD_STARTOPT_CLEAR_STATE

0x04 - ZCD_STARTOPT_AUTO_START

ZCD_NV_START_DELAY

Este parâmetro indica o atraso mínimo (em ms) depois de a função ser chamada.

ZCD_NV_EXTA_DDR

Este parâmetro contém o endereço IEEE do componente.

ZCD_NV_LOGICAL_TYPE

Este parâmetro indica o tipo lógico do componente. Pode ter um dos seguintes valores:

0X00 – ZG_DEVICETYPE_COORDINATOR

0X01 – ZG_DEVICETYPE_*ROUTER*

0X02 – ZG_DEVICETYPE_ENDDEVICE

Parâmetros de *poll*

Estes parâmetros são apenas aplicáveis a componentes do tipo *end device*s com pilhas.

ZCD_NV_POLL_RATE

Se este parâmetro tiver um valor diferente de 0 então o *end device* desperta periodicamente para verificar se o *router* seu pai tem dados para ele. O valor deste parâmetro corresponde ao valor do intervalo de tempo durante o qual o *end device* permanece em repouso (expresso em ms) e varia entre 1 e 65000.

Se o valor do parâmetro for nulo então o *end device* não acorda automaticamente para verificar se tem dados. Em vez disso, podem ser utilizados ou um *trigger* externo ou um evento interno para acordar o *end device*.

ZCD_NV_QUEUED_RATE

Quando um *end device* faz um poll e verifica junto do seu pai que tem dados, então o intervalo de tempo para o *poll* seguinte poderá ter uma menor duração. Esta característica é útil no caso de o *router* pai ter dados em espera para esse *end device*, podendo mesmo evitar que sejam perdidos dados.

Esta característica pode ser desligada colocando este valor a 0.

ZCD_NV_RESPONSE_POLL_RATE

Quando um *end device* envia um pacote de dados pode fazer o *poll* seguinte passado um intervalo de tempo de menor duração, no caso de a aplicação ficar a aguardar uma resposta. Esta característica não funciona se este valor estiver a 0.

ZCD_NV_POLL_FAILURE_RETRIES

Indica o número de vezes que o *end device* falha o contacto com o seu pai, antes de poder iniciar o mecanismo para procurar novo pai.

ZCD_NV_INDIRECT_MSG_TIMEOUT

Indica a quantidade de tempo (expressa em ms) que um *router* ou um coordenador guarda dados destinados a este *end device*. É recomendado que este valor seja no mínimo maior que a taxa de *poll*, de forma a garantir que o *end device* possa acordar e proceder ao *poll* dos dados.

Parâmetros de acknowledgement end-to-end

Acknowledges e retransmissões *end to end* apenas são aplicáveis se a aplicação o requisita explicitamente, quando envia um pacote de dados, ao activar o bit correspondente no parâmetro txOptions no call zb_SendDataRequest( ).

ZCD_NV_APS_FRAME_RETRIES

Indica o número de retransmissões efectuadas por um pacote de dados ao nível de aplicação, no caso de o pacote ser transmitido com a opção *acknowledge end to end* activada.

ZCD_NV_APS_ACK_WAIT_DURATION

Indica a quantidade de tempo (expressa em ms) que um componente deve esperar por um *acknowledge*, depois de transmitir um pacote com *acknowledge end to end*. Se o pacote não for recebido dentro desse intervalo de tempo, o componente emissor deve assumir falha e tentar uma retransmissão.

Outros parâmetros

ZCD_NV_BINDING_TIME

Indica a quantidade de tempo (expressa em ms) que um componente espera por uma resposta a um pedido de *binding*.

ZCD_NV_USERDESC

A este parâmetro correspondem 16 bytes opcionais (mais 1 de *overhead*) de dados definidos pelo utilizador, que podem ser configurados num componente, para que mais tarde ele possa ser facilmente descrito e/ou identificado.

A tabela seguinte resume as principais características dos parâmetros de configuração específicos do componente.

Tabela 4.11 - Resumo dos parâmetros de configuração específicos do componente

Parâmetro	configID	Tamanho (bytes)	Valor por defeito	Ficheiro
ZCD_NV_STARTUP_OPTION	0x0003	1	0	
ZCD_NV_START_DELAY	0x0004	1	START_DELAY	zglobals.c
ZCD_NV_EXTADDR	0x0004	8	DEVICE_LOGICAL_TYPE	zglobals.h
ZCD_NV_LOGICAL_TYPE	0x0084	1	Inválido (0xFFFF)	
ZCD_NV_POLL_RATE	0x0024	1	POLL_RATE	f8wconfig.cfg
ZCD_NV_QUEUED_RATE	0x0025	1	QUEUED_POLL_RATE	f8wconfig.cfg
ZCD_NV_RESPONSE_POLL_RATE	0x0026	1	RESPONSE_POLL_RATE	f8wconfig.cfg
ZCD_NV_POLL_FAILURE_RETRIES	0x0029	1	MAX_POLL_FAILURE_RETRIES	f8wconfig.cfg
ZCD_NV_INDIRECT_MSG_TIMEOUT	0x002b	1	NWK_INDIRECT_MSG_TIMEOUT	f8wconfig.cfg
ZCD_NV_*BINDING*_TIME	0x0046	2	APS_DEFAULT_MAX*BINDING*_TIME	zglobals.h
ZCD_NV_USERDESC	0x0081	17	0	

4.4.4 Comunicação entre o colector e o PC

A Evaluation Board utilizada no colector tem uma ligação USB e ainda uma ligação RS232.

A ligação USB ficou reservada para a alimentação da placa, enquanto a ligação RS232 foi utilizada na comunicação entre a mesma e o PC, para a transferência de dados. A configuração da comunicação série estabelecida entre o colector e o PC está registada na tabela 4.12.

Tabela 4.12 - Configuração da comunicação série estabelecida entre o colector e o PC

Taxa de transmissão	38400 bps
Bits de dados	8
Stop bits	1
Paridade	sem

Para a visualização dos dados é possível utilizar o Hiperterminal (Figura 4.14), ou o Z-Tool (Figura 4.15).
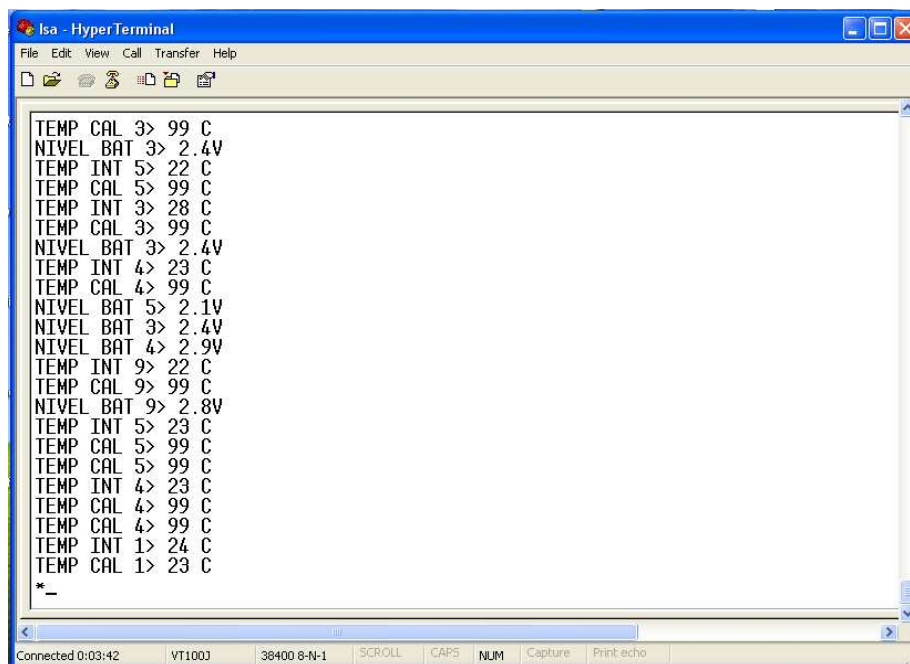
Figura 4.15 - Visualização dos dados recebidos no colector através do Hiperterminal
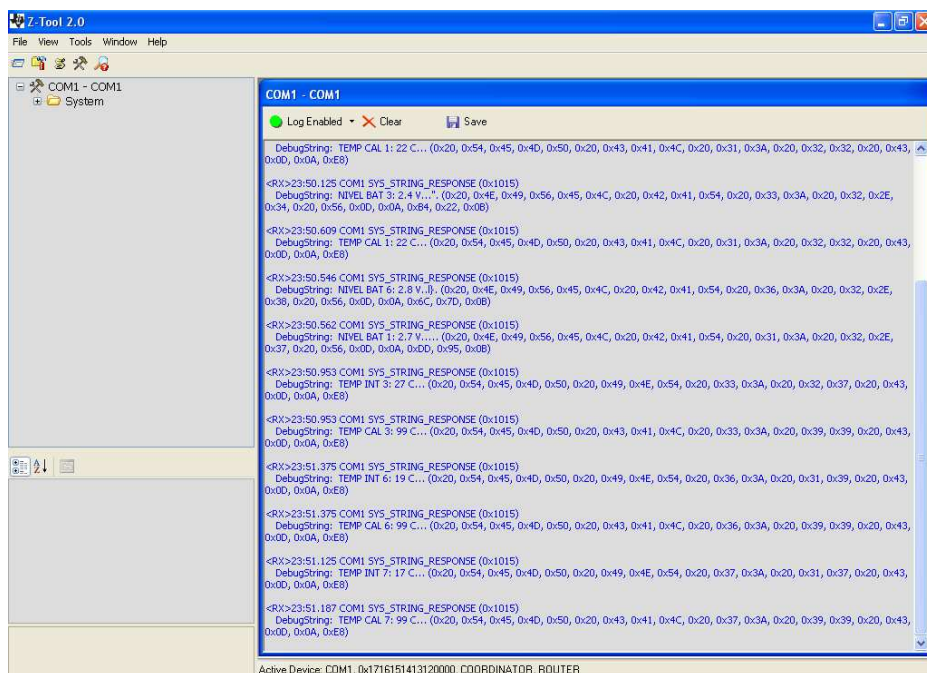
Figura 4.16 - Visualização dos dados recebidos no colector através do Z-Tool

O Z-Tool é um *software* fornecido com a Z-stack pela Texas Instruments, que permite, não só visualizar a recepção dos dados, como monitorizar os registos do módulo CC2431 inserido na Evaluation Board. A figura 4.17 ilustra a visualização dos registos do colector através do Z-Tool.
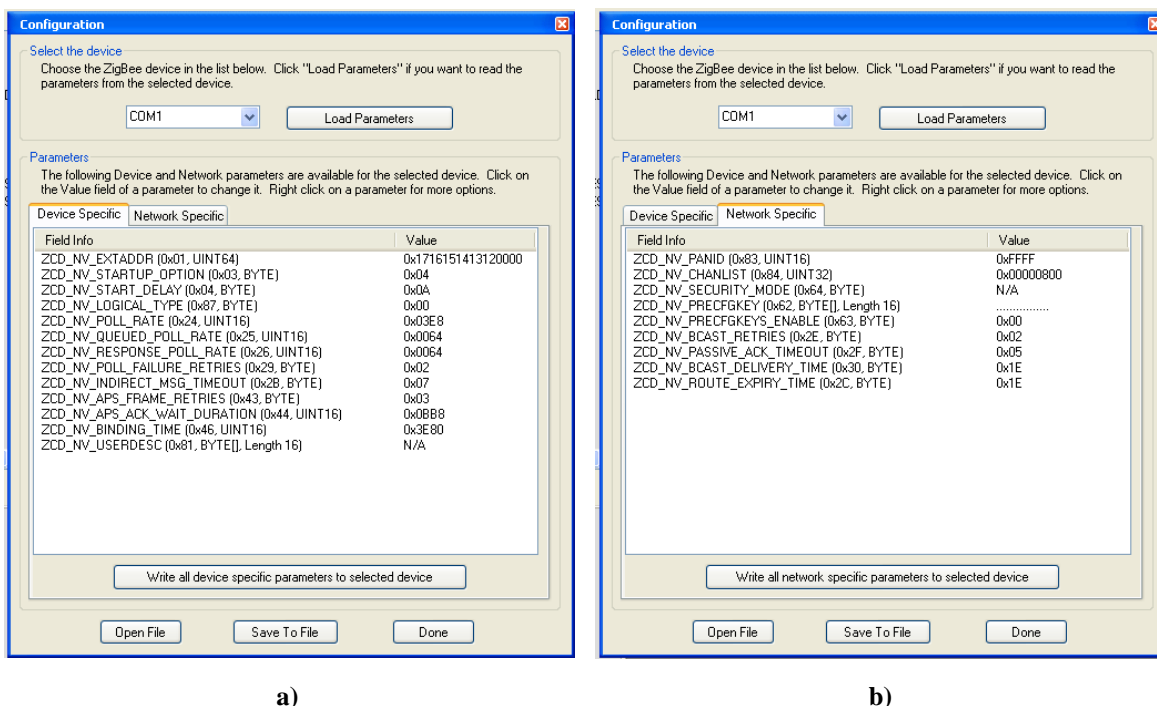
Figura 4.17 - Visualização dos registos do colector através do Z-Tool

a) específicos do colector b) específicos da rede

Na secção seguinte é efectuada uma análise aos resultados obtidos no projecto implementado.

4.5 Análise dos resultados obtidos

Numa primeira fase foi utilizado apenas um *end device* para validar, não só a comunicação baseada na Z-stack da Texas Instruments, mas também a utilização do sensor externo (Figura 4.18).

As periodicidades de monitorização das três variáveis foram as seguintes:

- Periodicidade de envio da temperatura medida com o sensor interno: 8 s;
- Periodicidade de envio do nível da bateria: 9 s;
- Periodicidade de envio da temperatura medida com o sensor externo: 11 s.

Com estes valores tentou-se evitar a possibilidade de coincidência temporal das tarefas.

a) **b)**
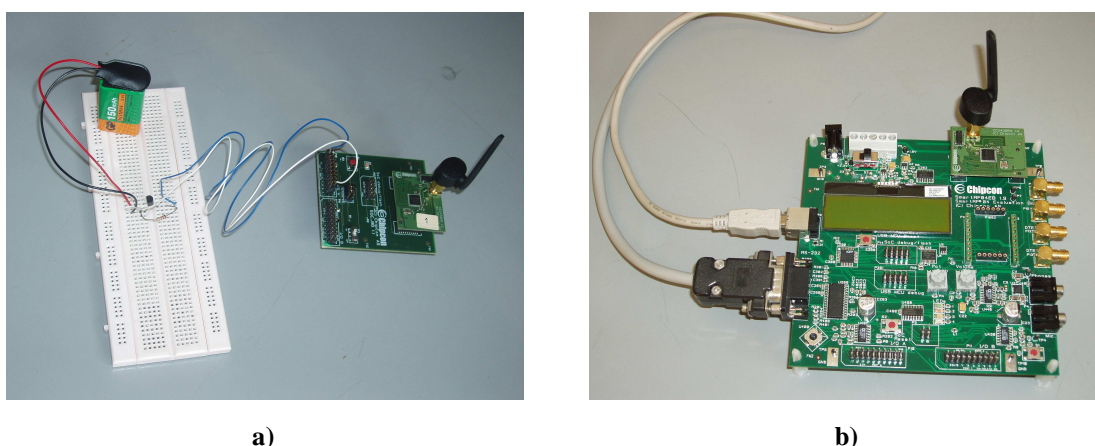
Figura 4.18 - Componentes da rede
a) end device b) colector

A validação da comunicação foi efectuada através das seguintes formas:

- Como o *end device* envia dados com pedido de *acknowledge end to end*, e caso não o receba desfaz o *bind* com o colector, então pode-se comprovar o sucesso da comunicação através da manutenção do *bind* por parte do *end device*;
- O colector está ligado via RS232 ao PC, sendo assim possível visualizar a recepção dos dados enviados pelo *end device*.

Quanto aos valores obtidos, comprovou-se a sua validade através das seguintes tarefas:

- Foram efectuadas medições entre os pinos VDD/3 e GND no SOC_BB, para confirmar os valores de nível de bateria obtidos no PC;
- Foram efectuadas medições à saída do sensor externo, para confirmar os valores obtidos no PC, tendo-se verificado a exactidão do sensor utilizado.
- No caso do sensor interno, foram utilizados como base de comparação os valores obtidos através do sensor de precisão, tendo-se verificado a necessidade de calibrar os sensores dos módulos CC2431, uma vez que os valores obtidos através dos sensores de temperatura internos diferiam dos obtidos através dos sensores externos. A calibração foi efectuada através do *software*, uma vez que este era o procedimento recomendado pelo fabricante.

De seguida foram acrescentados *end devices* à rede, até um número máximo de dez *end device*s (figura 4.19).
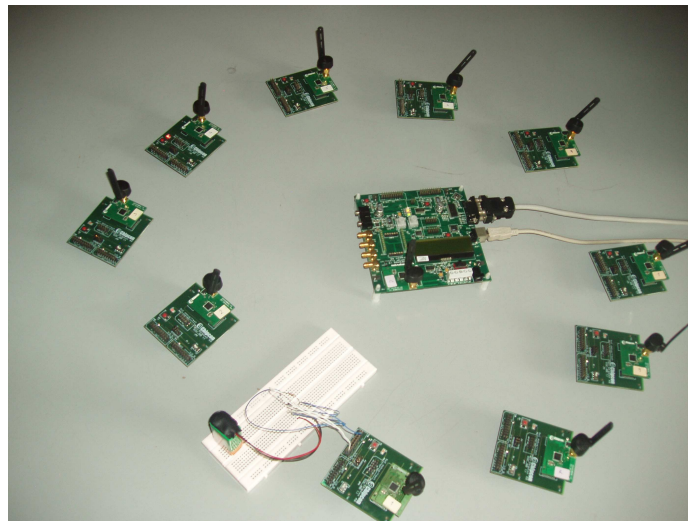
Figura 4.19 - Visualização dos vários componentes da rede

À medida que os *end device*s foram acrescentados, a partir de um total de cinco *end device*s, verificou-se que as frequências inicialmente estabelecidas eram demasiado elevadas, o que implicava perda de pacotes e consequente desfazer dos *bind*s por parte dos *end device*s.

Verificava-se ainda que estes últimos tentavam novo *bind* e, caso estivesse disponível outro colector (*router*), o *bind* era estabelecido com o segundo colector, o que permitia a recepção dos dados através de outro PC (figura 4.19). A possibilidade de um

segundo nó de instrumentação é um aspecto muito interessante ao nível da fiabilidade da rede implementada, pois através de redundância é possível garantir a monitorização permanente.
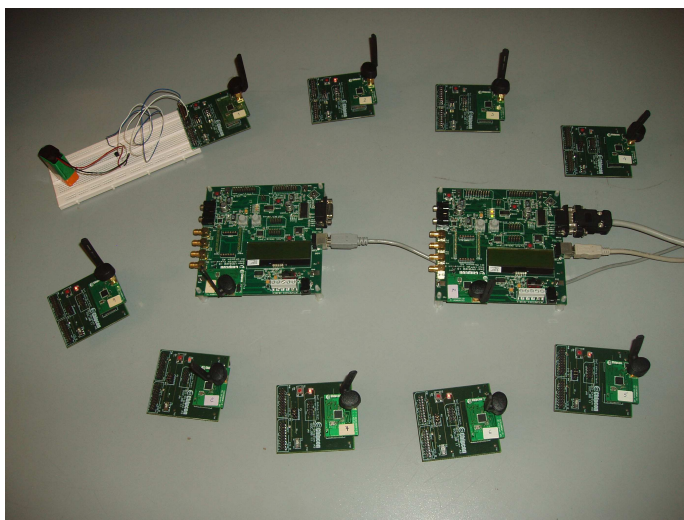
Figura 4.20 - Rede com dois colectores

Uma vez que as periodicidades iniciais se revelavam demasiado baixas para o número de componentes da rede, procedeu-se ao aumento progressivo das periodicidades até aos seguintes valores máximos:

- Periodicidade de envio da temperatura medida com o sensor interno: 50 s;
- Periodicidade de envio do nível da bateria: 60 s;
- Periodicidade de envio da temperatura medida com o sensor externo: 65 s.

Com estes valores foi verificada uma prestação mais eficiente da rede, uma vez que os *end device*s comunicavam com o colector, mantendo o *bind*, enquanto que no PC o fluxo de dados era suficiente para a monitorização das variáveis.

Poderiam até ser seleccionados valores mais elevados nas periodicidades de envio das variáveis monitorizadas, uma vez que se tratam de variáveis cuja variação ao longo do tempo é lenta, o que permitiria seleccionar intervalos de tempo entre monitorizações na ordem dos minutos. No entanto, como nesta fase do trabalho, o que se pretendia era testar a fiabilidade da rede no que respeita à transmissão dos dados, foram testados os cenários piores, que consistiam na selecção de baixas periodicidades.

Foram ainda estudados os seguintes aspectos: as distâncias entre *end device*s e o colector, bem como a possibilidade de localização de componentes da rede noutras divisões e utilização ao ar livre.

Relativamente às distâncias entre os *end device*s e o colector, os primeiros foram localizados em vários pontos da mesma divisão, com diferentes distâncias para o colector, desde uma distância mínima de 1 metro até uma distância máxima de 8 metros. Comprovou-se, não só a exactidão das medições, mas também a eficiência/qualidade da transmissão entre componentes de uma rede Zigbee até essa distância máxima e para a situação de espaço aberto, mas com a presença de barreiras físicas.

Verificou-se ainda que o tempo necessário para um *end device* estabeler o *bind* e iniciar a transmissão de dados era de 12 segundos (± 1 s), em qualquer das distâncias anteriormente referidas. O intervalo de tempo que decorria desde o estabelecimento do *bind* até à visualização dos primeiros dados no PC dependia da periodicidade definida, sendo no entanto independente da distância entre o *end device* e o colector, tal como no estabelecimento do *bind*. No caso das periodicidades mais baixas, decorriam 7 segundos, enquanto nas periodicidades mais altas demorava 49 segundos.

Procedeu-se à colocação de *end device*s noutras divisões, mas nesses casos a comunicação falhou a 12 metros de distância. No entanto, para a mesma distância e no caso de duas divisões contíguas, bastou manter a porta aberta para a comunicação se estabelecer, verificando-se que não era um *blind spot*.

Procedeu-se ainda à colocação dos vários elementos da rede ao ar livre. Nessa situação verificou-se que a distância de transmissão suportada pela rede era muito maior do que nas situações anteriores, o que seria de esperar, uma vez que não existiam tantas barreiras físicas, logo não havia tanta atenuação do sinal RF.

Verificou-se assim que a *performance* da comunicação entre os *end device*s e o colector depende das barreiras físicas e dos fenómenos de reflexão, refracção e espalhamento, sendo superior no caso de funcionamento em espaço aberto.

4.6 Conclusão

A utilização de uma arquitectura sem fios justifica-se pelas necessidades crescentes na realização de instrumentação/controlo de locais remotos, onde a cablagem do local se torne demasiado cara e/ou de difícil execução. Também a crescente mobilidade e o

estabelecimento de ligações com os mais diversos dispositivos de uma forma transparente para o utilizador são aspectos fundamentais para a emergência das redes sem fios.

Com a rápida evolução dos mercados a flexibilidade e a adaptabilidade dos processos produtivos são cada vez mais um imperativo, que encontra nas arquitecturas de redes sem fios um óptimo aliado.

Neste capítulo procedeu-se à descrição do funcionamento do sistema de instrumentação distribuída suportado por uma rede sem fios.

Ficou demonstrada, não só a flexibilidade/facilidade da criação de uma rede Zigbee, mas também a integração de vários pontos com leituras de vários sensores.

Verificou-se no entanto que deverá haver um bom equilíbrio entre a quantidade de dados a enviar, a periodicidade do envio de dados e o número de dispositivos ligados ao mesmo colector, sendo aconselhável a utilização de redundâncias (totais ou parciais) de modo a garantir a fiabilidade da rede.

A universalidade da comunicação sem fios entre os vários dispositivos, assente na utilização do protocolo IEEE 802.15.4/Zigbee, garante a este projecto um elemento integrador e universal na área da instrumentação remota sem fios.

No capítulo seguinte é efectuada uma análise aos resultados obtidos no projecto desenvolvido, sendo ainda apresentadas algumas perspectivas para desenvolvimentos futuros.

5 Conclusão

A comunicação sem fios é uma das tecnologias de comunicações em grande expansão. Esta permite uma grande mobilidade e uma grande interactividade entre os mais diversos dispositivos ou sistemas. No entanto, esses factores diferenciadores, geradores de valor acrescentado relativamente às outras tecnologias, levantam desafios que é necessário ultrapassar.

A comunicação sem fios no chão de fábrica não só permite uma maior flexibilidade na instalação, manutenção e actualização, como suprime os problemas devidos à cablagem. No entanto, um sistema de comunicação sem fios para operar no chão de fábrica de um modo eficiente tem de garantir as seguintes características: suporte de um grande número de sensores e actuadores, baixo consumo, baixo e previsível atraso na transferência de dados e elevada fiabilidade.

Até agora as tecnologias sem fios ainda não ganharam grande aceitação no chão de fábrica. Uma das principais razões é a dificuldade em conseguir uma transmissão em tempo real bem sucedida em canais propensos a erros. Nos ambientes industriais os factores que contribuem para a degradação dos canais de comunicação sem fios consistem na presença de motores eléctricos e de uma variedade de equipamentos que provocam descargas eléctricas, o que contribui para um nível elevado de erros nos bits e de perdas de pacotes de dados. A melhoria da qualidade do canal de comunicação e o desenvolvimento de aplicações robustas e tolerantes a falhas são aspectos que contribuem significativamente para a aceitação de tecnologias sem fios em aplicações industriais.

Neste trabalho foi analisado o estado da arte das redes de comunicação industriais, sendo dado particular destaque aos *standards* sem fios, tendo em vista a aplicação de um *standard* deste tipo, o IEEE 802.15.4/Zigbee, para o desenvolvimento de um sistema de instrumentação distribuída suportado numa rede sem fios.

No capítulo 2, Redes de Comunicações Industriais, foi abordado o estado da arte das redes de comunicações industriais.

No capítulo 3, Redes de Comunicações Sem Fios, foi analisado o estado da arte das redes de comunicações sem fios, tendo sido abordados os *standards* mais implementados, com vista à escolha do *standard* a ser utilizado no projecto.

No capítulo 4, Sistema de Instrumentação Distribuída Suportado Por Rede Sem Fios, foi apresentado o trabalho desenvolvido, baseado no *standard* de comunicação sem fios IEEE 802.15.4/Zigbee e na plataforma de hardware CC2431 da Chipcon/Texas Instruments.

Através do estudo das redes de comunicação industriais, com particular destaque nas redes de comunicação sem fios, foi seleccionado o *standard* IEEE 802.15.4/Zigbee, que, devido ao baixo consumo energético e boa escalabilidade, permite redes com grande potencial na implementação de nós de instrumentação distribuídos.

No trabalho desenvolvido foi utilizado o CC2431 Development Kit da Chipcon/Texas Instruments.

Entre os resultados obtidos na elaboração deste trabalho, importa destacar os seguintes:

- Confirmação da tendência do mercado na evolução de soluções baseadas em comunicações sem fios.
- Contacto com diversas plataformas de standards sem fios existentes no mercado.
- Comparação entre as diversas tecnologias de comunicação sem fios nos seguintes domínios: mercado alvo, distância máxima de comunicação, tamanho da rede, tamanho dos pacotes transmitidos, taxa de transferência e segurança na transmissão de dados.
- Identificação de problemas existentes ao nível da implementação de sistemas baseados em tecnologias de comunicação sem fios.
- Contacto com diversas ferramentas no desenvolvimento do trabalho.
- Confirmação da necessidade de criação de um standard de comunicações sem fios destinado aos processos de monitorização e controlo em ambiente industrial.

Desenvolvimentos futuros

O desenvolvimento de um sistema de instrumentação distribuída suportado por rede sem fios é uma tarefa multidisciplinar, que envolve áreas de conhecimento distintas.

Devido ao carácter multidisciplinar deste trabalho, a dispersão nas fontes de informação em qualquer das áreas é bastante elevada. No entanto, tentou-se abranger todas as áreas envolvidas.

De seguida são apresentados alguns aspectos que constituem linhas de orientação para futuros trabalhos e desenvolvimentos em algumas das áreas abordadas neste trabalho:

- Com vista a completar a malha de controlo, integrar actuadores com controlo local e/ou distribuído.
- Desenvolvimento de um software para monitorização e/ou controlo remotos e armazenamento de dados.
- O módulo CC2431 inclui suporte para a função *Location Engine*. O Location Engine permite determinar a localização de um nó da rede. A integração desta função não só permitiria a calibração de cada nó sensor de uma forma transparente, mas também possibilitaria a utilização de nós sensores móveis para aquisição de dados em vários pontos espacialmente distribuídos.
- Explorar as possibilidades de gestão de energia do CC2431, de modo a optimizar a eficiência energética do sistema desenvolvido.
- Análise da rede Zigbee, com recurso a *software* analisador de redes, como o Daintree da Daintree Networks.
- Análise de custo/benefício entre a optimização da comunicação, utilizando uma topologia hierárquica e a consequente perda de flexibilidade.
- Estudo de aspectos relacionados com a confiança da rede: fiabilidade, disponibilidade, manutibilidade e segurança.

Existem muitas oportunidades de investigação no campo das comunicações industriais sem fios, sendo de destacar as seguintes:

- A procura de novos mecanismos de protocolo cujo objectivo consiste na melhoria da *performance* em tempo real. Um componente chave no *design* e na avaliação

de tais mecanismos é a formulação de medidas de *performance* apropriadas a aplicações de *benchmarking* e modelos de canais sem fios adaptados a ambientes industriais.

- A avaliação das várias tecnologias sem fios emergentes, tanto do ponto de vista tecnológico, como do ponto de vista do mercado, tendo em vista a sua potencial utilização em aplicações industriais.
- Outras áreas de investigação envolvem aspectos como a segurança, o apoio à mobilidade e ainda o objectivo comum de transmissão em tempo real e eficiência energética.

Bibliografia

[1] R. Zurawski, The Industrial Communication Technology Handbook, CRC Press, 2005

[2] R. Zurawski, Special Issue on Industrial Communication Systems, Proceedings of the IEEE, Vol. 93, No. 6, pp. 1067-1072, June 2005

[3] P. Neumann, Communication in Industrial Automation – What is going on, Control Engineering Practice, 15, pp.1332-1347, 2007

[4] H. Kopetz, Real-Time Systems: Design Principles for Distributed Embedded Applications, Kluwer Academic Publishers, 1997

[5] P. Portugal, Avaliação da Confiança no Funcionamento de Redes de Campo, Tese de Doutoramento, Faculdade de Engenharia da Universidade do Porto, Setembro 2004

[6] D. Heffernan, A Technical Overview of Fieldbus Developments from Origins to Present Day Standards, Technical Report, Department of Electronic and Computer Engineering, University of Limerick, 1997

[7] M. Felser, The Fieldbus Standards: History and Structures, Technology Leadership Day, Microswiss Network, HTA Luzern, 10 October 2002

[8] C. Rameback, Process Automation Systems - History and Future, IEEE International Conference on Emerging Technologies and Factory Automation, 2003

[9] M. Alves, Real-Time Communications over Hybrid Wired/Wireless PROFIBUS-Based Networks, Tese de Doutoramento, Faculdade de Engenharia da Universidade do Porto, 2003

[10] A. Willig, Wireless LAN Technology for the Factory Floor, The Industrial Information Technology Handbook, CRC Press, 2004

[11] T. Bangemann, Management of distributed Automation Systems Based on Web Technologies, International Conference on Fieldbus Systems and their Applications, 2001

[12] R. Patzke, Fieldbus Basics, Computer Standards & Interfaces, Vol. 19, 1998

[13] H. Schumny, Fieldbuses in Measurement and Control, Computer Standards & Interfaces, Vol. 19, pp. 295-304, 1998

[14] E. Tovar, Tese de Mestrado, Faculdade de Engenharia da Universidade do Porto, 1999

[15] J. R. Pimentel, Communication Networks for Manufacturing, Prentice-Hall, 1990

[16] J. P. Thomesse, A Review of the Fieldbuses, Annual Reviews in Control, Vol. 22, pp. 35-45, 1998

[17] J. P. Thomesse, Fieldbuses and interoperability, Control Engineering Practice, Vol. 7, pp. 81-94, 1999

[18] M. Felser, Real-Time Ethernet – Industry Prospective, Proceedings of the IEEE, Vol. 93, No. 6, pp. 1118-1129, June 2005

[19] Sirkka-Liisa, Jamsa-Jounela, Future Trends in Process Automation, Annual Reviews in Control, 2007

[20] G. Fernandes, Análise e Desenvolvimento de Comunicação e Computação Móvel em Sistemas de Automação, Tese de Mestrado, FEUP, Fevereiro 2004

[21] A. Willig et al, Wireless Technology in Industrial Networks, Proceedings of the IEEE, Vol. 93, No. 6, pp. 1130-1151, June 2005

[22] Palowireless, Bluetooth Resource Center, 2007

[23] I. Howitz et al, Empirical Study for IEEE 802.11 and Bluetooth Interoperability, Proceedings of the IEEE Vehicular Technology Conference, Vol. 2, No. 6, pp. 1109-1113, 2001

[24] I. F. Akyildiz, W. Su, Y. Sankarasubramanian, E. Cayirci, Wireless Sensor Networks: a survey, Computer Networks, 38, pp. 393-422, 2002

[25] When everything connects, The economist, April 28, 2007

[26] Zigbee Alliance, 2008

[27] Zigbee Specification, document number 053474r17, 2007

[28] Zigbee Technology, document number 051418r, 2 October 2003

[29] Zigbee Alliance Overview, document number 075482r00, 2007

[30] A. Cunha, On the use of IEEE 802.15.4/Zigbee as Federating Communication Protocols for Wireless Sensor Networks, Tese de Mestrado, FEUP, Julho 2007

[31] CC1110DK/CC2430DK/CC2510DK User Manual (Rev. 1.5), document number SWRU039, Texas Instruments, Inc., 2005

[32] CC2430 Data Sheet (Rev. 2.1), document number SWRS036F, Texas Instruments, Inc. 2005

[33] CC2431 Data Sheet (Rev. 2.01), document number SWRS034B, Texas Instruments, Inc., 2005

[34] Z-Stack User's Guide for CC2431ZDK, document number F8W-2006-0025, Texas Instruments, Inc., 2005

[35] Application note: Create New Application for the CC2430DB, document number F8W-2005-0033, Texas Instruments, Inc., 2005

[36] Z-Stack Compile Options, document number F8W-2005-0038, Texas Instruments, Inc., 2005

[37] Z-Stack Sample Applications, document number F8W-2006-0023, Texas Instruments, Inc., 2006

[38] Z-Stack Sample Application for CC2430DB, document number F8W-2006-0023, Texas Instruments, Inc., 2006

[39] Simple API for Z-Stack, document number F8W-2007-0021, Texas Instruments, Inc., 2007

[40] Application note: Power Management for the CC2430DB, document number F8W-2006-0019, Texas Instruments, Inc., 2006

[41] IAR IDE User Manual (Rev. 1.2), document number SWRU038, Texas Instruments, 2005

[42] IAR Embedded Workbench IDE User Guide, Third Edition, December 2004

[43] 8051 IAR C/C++ Compiler Reference Guide, Third Edition, July 2005

[44] W. Kester, Data Conversion Handbook, Elsevier, 2005

[45] U. Beis, An Introduction to Delta Sigma Converters, 2008

[46] LM35 Precision Centigrade Temperature Sensors, document number DS005516, National Semiconductors, November 2000